EXHIBIT 11
Public Version—Redacted

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
San Francisco Division

NETWORK PROTECTION SCIENCES, LLC,	§	
Plaintiff,	§	
v.	§	
	§	Civil Action No.
FORTINET, INC.,	§	3:12-CV-01106-WHA
Defendant.	§	

EXPERT REPORT
OF
JOHN C. JAROSZ

July 3, 2013

I. INTRODUCTION

A. Assignment

I, John C. Jarosz, submit this expert report on behalf of Network Protection Sciences, LLC ("NPS") in the above-captioned case. I have been retained by NPS to provide expert analysis and testimony, if necessary, regarding damages that NPS may have sustained due to the alleged infringement of U.S. Patent No. 5,623,601 ("the '601 patent") by Fortinet, Inc. ("Fortinet"). For purposes of assessing damages in this case, I have assumed that the '601 patent will be found valid, enforceable, and infringed by Fortinet's accused products.

This report is based on the information that was available to me as of the date of this report. I reserve the right to revise, supplement, or expand my opinions prior to trial, if necessary, based on further review and analysis of information provided to me subsequent to the filing of this report.

B. Summary of Conclusions

Based on my analysis of the evidence from the Market Approach, Income Approach, and Cost Approach, and application of the *Georgia-Pacific* factors, it is my opinion that NPS is entitled to reasonable royalty damages based on a running royalty rate of 4 percent. When applied to U.S. sales of accused hardware and virtual machines, damages total $6.8 million; when applied to U.S. sales of convoyed sales of bundled services and service renewals, damages total $6.4 million.[1] Damages associated with estimated sales in Canada and Latin America total $2.4 million for accused hardware and virtual machines and $2.4 million for convoyed sales of bundled services and service renewals.[2] These amounts assume a finding of liability for at least one claim of the patent-in-suit. Total damages when applied to sales of accused hardware and virtual machines and associated services in the U.S., Canada, and Latin America are $18.1 million.[3]

---

1 Tab 3.

2 Tab 3. Calculations based on estimated sales in Canada and Latin America. If Fortinet produces information regarding actual sales of accused products and associated services in Canada and Latin America, I will update my calculations accordingly.

3 Tab 3.

C. Qualifications

I am a Managing Principal of Analysis Group, Inc. ("AG") and Director of the firm's Washington, DC office. Analysis Group, Inc. is an economic, financial and strategy consulting firm with offices in Beijing, China; Boston, MA; Chicago, IL; Dallas, TX; Denver, CO; Los Angeles, CA; Menlo Park, CA; Montreal, Quebec; New York, NY; San Francisco, CA; and Washington, DC. We provide research and analysis in a variety of business, litigation and regulatory matters, and have particular expertise in intellectual property ("IP") matters, having been engaged in numerous cases involving patents, copyrights, trademarks, trade secrets and unfair competition.

I am an economist whose specialty is IP valuation and monetary relief assessment. I have been involved in more than 300 such engagements spanning a broad range of industries, including computer and telecommunications hardware and software. My resume is attached as Tab 1. It describes all of my testimony (either in deposition or at trial) and all of my publications.

D. Evidence Considered

In undertaking my study, I have considered information from a variety of sources, each of which is a type that is reasonably relied upon by experts in my field. Those sources are identified in Tab 2. In addition, I have spoken with NPS's technical expert, Angelos Keromytis. I also have relied upon my professional judgment and expertise, gathered from many years of estimating damages and valuing technology in intellectual property contexts.

E. Compensation

My firm has billed NPS on a time-and-materials basis for my work and that of my colleagues. My hourly billing rate for the time spent consulting and calculating damages, which includes my study of pertinent issues and materials, is $620. I also have directed the efforts of other staff members of AG, whose hourly billing rates range from $195 to $445. This compensation is not, in any way, dependent on the outcome of this proceeding or the substance of my opinion.

II. BACKGROUND

A. Parties-In-Suit

1. Network Protection Sciences, LLC.

NPS is a Texas Limited Liability Company based in Longview, Texas[4] and is a subsidiary of Unifi Scientific Advances, Inc. ("Unifi Scientific").[5] According to its website, Unifi Scientific, also based in Longview, Texas, is a company that "couple[s] technology expertise and real-world experience to support the growth of underlying and parallel business opportunities" and commercializes intellectual property assets.[6]

2. Fortinet, Inc.

Founded in 2000, Fortinet is a Sunnyvale, California based company[7] that provides "network security solutions that are designed to address the fundamental problems of an increasingly bandwidth-intensive network environment and a more sophisticated information technology ('IT') threat landscape."[8] As of December 31, 2012, Fortinet employed 1,954 people, worldwide, and it reported $533.6 million in revenue and $66.8 million in net income in FY 2012.[9] Fortinet revenues generated in the United States totaled $145.4 million in 2012, accounting for 27.2 percent of its worldwide revenues.[10]

Fortinet's core products include FortiGate Unified Threat Management ("UTM")/Next Generation Firewall ("NGFW") products along with the FortiManager central management and FortiAnalyzer central logging and reporting products.[11] FortiManager and FortiAnalyzer products "are typically purchased to compliment a large FortiGate deployment."[12] The FortiGate products run the FortiOS software, which "provides the foundation for the operation of all FortiGate appliances…[and]

---

4 Plaintiff's Original Complaint for Patent Infringement, July 6, 2010 ("Complaint"), at ¶ 1.
5 http://www.unifiscientific.com/index.php?option=com_content&view=article&id=53 (viewed June 5, 2013).
6 http://www.unifiscientific.com/index.php?option=com_content&view=article&id=49&Itemid=55 (viewed June 5, 2013).
7 http://www.fortinet.com/aboutus/aboutus.html (viewed June 5, 2013).
8 FORT-NPS 148967 – 9079, at 8971.
9 FORT-NPS 148967 – 9079, at 8978, 9002; Tab 4.
10 FORT-NPS 148967 – 9079, at 9062; Tab 6.
11 FORT-NPS 148967 – 9079, at 8973.
12 FORT-NPS 148967 – 9079, at 8973.

provides multiple layers of security."[13] Fortinet virtual appliances[14] are also available for the FortiGate, FortiManager, FortiAnalyzer, and other Fortinet products.[15] According to Fortinet, "[t]hese virtual appliances help secure network infrastructures with the same functionality as the traditional physical appliances in their respective product lines."[16] Fortinet's product revenues, which included the sale of physical and virtual appliances, totaled nearly [redacted] in 2012, and, over the 2004 through 2012 period represented approximately [redacted] of total Fortinet revenues.[17]

Fortinet provides a variety of FortiGuard security subscription services, which provide security updates, such as antivirus and anti-spam updates, directly to end-customers; FortiCare technical support services, which provides technical support to end-customers related to software, firmware, and hardware; training services; and professional services, which includes assistance with the design and deployment of products.[18] Fortinet's service revenues totaled over [redacted] in 2012, and, over the 2004 through 2012 period, represented approximately [redacted] of total Fortinet revenues.[19] The remaining revenues were classified as ratable products and services.[20]

B. Network Security and Unified Threat Management

1. Overview of Network Structure

The Open System Interconnection ("OSI") model is the most common framework for the design

---

13 FORT-NPS 148967 – 9079, at 8972.

14 "A virtual appliance is a virtual machine image file consisting of a preconfigured operating system environment and a single application. The purpose of a virtual appliance is to simplify delivery and operation of the application." *See*, http://www.searchservervirtualization.com/definition/virtual-appliance (viewed July 3, 2013). "A virtual machine (VM) is a software implementation of a computing environment in which an operating system (OS) or program can be installed and run. The virtual machine typically emulates a physical computing environment, but requests for CPU, memory, hard disk, network and other hardware resources are managed by a virtualization layer which translates these requests to the underlying physical hardware." *See*, http://www.searchservervirtualization.com/definition/virtual-machine (viewed July 1, 2013).

15 FORT-NPS 148967-9079, at 8971.

16 FORT-NPS 148967-9079, at 8971.

17 Tab 4.

18 FORT-NPS 148967-9079, at 8975-6.

19 Tab 4.

20 Tab 4. Fortinet's annual report states that "[r]atable and other revenue is generated from sales of our products and services in cases where the fair value of the services being provided cannot be separated from the value of the entire sale….In fiscal 2012 and 2011, this category includes a $3.7 million and a $2.6 million sale of previously acquired patents, respectively." *See*, FORT-NPS 148967-9079 , at 9009

of network models.[21] The OSI model consists of several layers that describe how information moves from an application running on one computer to an application running on another networked computer.[22] The seven layers of the OSI model, from lowest to highest, are the physical layer,[23] the data link layer,[24] the network layer,[25] the transport layer,[26] the session layer,[27] the presentation layer,[28] and the application layer.[29] The lower layers (layers 1 to 4) ensure "that the data gets to where it needs to go reliably," and the upper layers (layers 5 to 7) of the OSI network model "are concerned mainly with user interaction and the implementation of software applications, protocols and services that let us actually make use of the network."[30]

2. Overview of Network Security and Unified Threat Management

Network security systems have evolved over time from the single-featured firewall, which filters network traffic to promote security,[31] to multi-featured UTM and NGFW systems.[32] A firewall was traditionally "an in-line security control that implements network security policy between networks of

---

21 http://www.tcpipguide.com/free/t_TheOpenSystemInterconnectionOSIReferenceModel.htm (viewed July 1, 2013).

22 http://www.tcpipguide.com/free/t_TheOpenSystemInterconnectionOSIReferenceModel.htm (viewed July 1, 2013).

23 The physical layer (layer 1) "is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium." *See*, http://support.microsoft.com/kb/103884 (viewed July 1, 2013).

24 The data link layer (layer 2), "provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link." See, http://support.microsoft.com/kb/103884 (viewed July 1, 2013).

25 The network layer (layer 3) decides "which physical path the data should take based on network conditions." *See*, http://support.microsoft.com/kb/103884 (viewed June 29, 2013).

26 The transport layer (layer 4) "ensures that messages are delivered error-free, in sequence, and with no loss or duplications." *See*, http://support.microsoft.com/kb/103884 (viewed June 29, 2013).

27 The session layer (layer 5) "allows two application processes on different machines to establish, use and terminate a connection, called a session," and it "performs the functions that allow these processes to communicate over the network." *See*, http://support.microsoft.com/kb/103884 (viewed June 29, 2013).

28 The presentation layer (layer 6) "takes data provided by the Application layer and converts it into a standard format that other layers understand." *See*, http://support.microsoft.com/kb/103884 (viewed June 29, 2013).

29 The application layer (layer 7) "is the layer that actually interacts with the operating system or application whenever the user chooses to transfer files, read messages or perform network-related activities." *See*, http://support.microsoft.com/kb/103884 (viewed June 29, 2013).

30 http://www.tcpipguide.com/free/t_UpperLayerLayers56and7NetworkingProtocolsServicesa.htm (viewed June 29, 2013).

31 FORT-NPS 144131-64.

32 UTM and NGFW are similar. I understand that NGFWs provide a subset of UTM functions. *See*, Bedwell Exhibit 42, at 46.

different trust levels in real time."[33] "Traditional or 'first-generation' firewalls rely on port numbers or protocol identifiers to recognize and categorize network traffic and enforce policies related to such traffic."[34] I understand that the traditional firewall is able to identify different types of applications based on the ports that they utilize and selectively apply policies to traffic on those ports, but it is unable to distinguish between multiple types of applications flowing through a single port.[35] The proliferation of web-based applications increased the number of and variety of browser-based applications, posing challenges for traditional firewalls and increasing risks to network security.[36]

UTM emerged around 2004 in response to increasingly complex network security threats.[37] UTM appliances are, broadly speaking, network security solutions, a category that includes other firewall products, virtual private network products ("VPN"), and network intrusion detection and prevention systems.[38] Modern network security devices provide security at multiple layers of the network,[39] and I understand that many UTM functions operate at the application layer.

UTM products consolidate multiple security technologies into a single appliance.[40] Before UTMs, network administrators managed disjoint security appliances for essential functions such as network firewall, network intrusion prevention, anti-malware, anti-spam, virtual private network, content-filtering, and load-balancing.[41] This security structure was expensive, inefficient, slow, and wasted physical space. By consolidating these functions, UTM appliances allow higher value, in terms of space and efficiency, at a lower cost to consumers.[42]

---

33 John Pescatore and Greg Young, Gartner, "Defining the Next-Generation Firewall," October 12, 2009, at 2.
34 Bedwell Exhibit 45, at 11.
35 Bedwell Exhibit 45, at 12.
36 Bedwell Exhibit 45, at 11-14.
37 FORT-NPS 146680-774, at 685.
38 FORT-NPS 144131-64, at 31.
39 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/DN1246_nemertes_firewall_evolution.pdf (viewed June 29, 2013).
40 FORT-NPS 146817-934, at 821.
41 FORT-NPS 146031-125, at 036.
42 FORT-NPS 146031-125, at 036.

Third-party estimates of UTM or network security revenues vary based on the specific marketplace being evaluated.[43] According to IDC, worldwide UTM sales totaled $1.29 billion in 2007, accounting for 21.0 percent of the $6.15 billion in worldwide network security revenues in 2007.[44] By 2011, IDC indicated that worldwide UTM grew to $2.2 billion, accounting for 30.2 percent of the $7.4 billion in worldwide network security revenues, and it forecasted that by 2016, worldwide UTM revenues will total $4.3 billion, equal to 42.6 percent of the forecasted $10.1 billion in worldwide network security revenues.[45] Frost & Sullivan reported 2011 worldwide UTM revenues of $1.3 billion and forecasted UTM revenues to grow to $2.8 billion by 2016.[46]

According to IDC, Fortinet (16.8 percent), Check Point (12.8 percent), and Juniper Networks (8.5 percent) were the three largest companies in the worldwide UTM marketplace in 2011.[47] According to Frost & Sullivan, Fortinet (20.5 percent), Check Point (14.7 percent), and Cisco (13.7 percent) were the three highest selling UTM companies worldwide in 2011.[48]

3. UTM Functions

As noted above, UTMs consolidate several features and capabilities into a single device. The core functions of a UTM include firewalls, intrusion prevention services ("IPS"), application control, virtual private network, content filtering, IPv6 support, and support for virtualized environments.[49] UTMs also allow users to deploy data loss prevention ("DLP"), anti-virus and anti-spam protection, endpoint control, and integrated wireless local area networks ("WLAN").[50] UTMs also can provide secure socket

---

43 The market research company IDC defines UTM as security products that include multiple features integrated into one device, which may include NGFW products. *See*, FORT-NPS 144131-64, at 35. Gartner, Inc., another market research company, defines UTM as multifunction network security products used by small or midsize businesses. *See*, FORT-NPS 144126-130, at 30. Frost & Sullivan defines UTM as a multi-function, next generation firewall solution that is optimized for small and medium sized businesses. *See*, FORT-NPS 146817-934, at 827.

44 FORT-NPS 144131-64, at 48.

45 FORT-NPS 144131-64, at 48.

46 FORT-NPS 146817-934, at 846.

47 FORT-NPS 144131-164, at 41-42.

48 FORT-NPS 146817-934, at 857.

49 Bedwell Exhibit 45, at 26.

50 Bedwell Exhibit 45, at 26-27.

layer ("SSL")-encrypted traffic inspection.[51] These various functions are described below.

- **Firewall** – Firewall products primarily function as general-purpose filters for network traffic; firewalls may inspect network traffic using stateful inspection or deep packet inspection ("DPI").[52] Stateful inspection provides a "set of rules to allow or deny connections based on source and destination IP address, port and user profile."[53] DPI goes beyond stateful inspection by inspecting the data within a packet as it passes an inspection point, searching for defined criteria, such as virus, spam, or other intrusions.[54]
- **IPS –** IPS refers to a set of signatures that are applied to traffic streams to block worms and targeted attacks.[55]
- **Application Control** – Application control makes it possible to selectively block, allow or restrict access to individual applications.[56]
- **VPN** – VPNs allow organizations to use encryption and authentication to extend their network's secure connectivity to remote offices or users.[57]
- **Content Filtering –** Content filtering allows a "large set of predetermined classifications of Web addresses to prevent employee abuse of the Web, as well as to block access to malicious URLs."[58]
- **IPv6 Support** – IPv6 support allows appliances to recognize the latest revision of the Internet Protocol, the communications protocol allowing computers to identify and locate systems on networks and internet traffic routes.[59]
- **Virtual Domains** – Virtual domains allow the appliance to function as multiple independent units

---

51 FORT-NPS 000025-31, at 29.
52 FORT-NPS 144131-64, at 35.
53 FORT-NPS 145346-61, at 49.
54 http://www.techopedia.com/definition/24973/deep-packet-inspection-dpi (viewed June 26, 2013).
55 FORT-NPS 145346-61, at 49.
56 http://docs.fortinet.com/fgt/ifos/inside-fortios-appcntrl-40-mr3.pdf (viewed June 26, 2013).
57 FORT-NPS 144131-64, at 36.
58 FORT-NPS 145346-61, at 49.
59 http://www.fortinet.com/resource_center/solution_briefs/ipv6_and_fortinet_network_security_next_generation_ip_communication (viewed June 26, 2013).

with common administration.[60] Virtual Local Area Networks increase the number of network interfaces beyond the physical connections on the unit.[61]

- **DLP** –DLP is a method of identifying and monitoring sensitive data that reduces data leaks and restricts unauthorized access.[62]
- **Anti-virus and Anti-spam –** Anti-virus software detects, prevents, and destroys computer viruses and other malware,[63] and anti-spam refers to methods that detect spam, which are emails with unsolicited advertisements.[64]
- **Endpoint Controls –** Endpoint controls are designed to reduce risks from users that access the network from riskier environments like kiosks, wireless hot spots, private PCs, and unmanaged PDAs.[65]
- **WLAN** – WLAN refers to a wireless distribution method for two or more devices.[66]
- **SSL-Encrypted Traffic Inspection** – SSL-encrypted traffic inspection is a method of protection for endpoint users against hidden threats that intercepts threats before routing encrypted traffic to its final destination.[67]

4. Transparent Application Layer Proxies

It is my understanding that a transparent application layer proxy is a type of firewall and represents an improvement over prior firewall technologies because 1) it accurately reconstructs information coming through the firewall in a manner that allows the firewall to more effectively block the passage of unwanted data relative to other methods of doing so, and 2) it does not require the system to be separately configured by a user or system administrator in order to accommodate each individual user that

---

60 http://docs.fortinet.com/fgt/archives/2.8MR7/01-28007-009120050401_FortiGate_VLANs_and_VDOMs_Guide.pdf (viewed June 25, 2013).

61 http://docs.fortinet.com/fgt/archives/2.8MR7/01-28007-009120050401_FortiGate_VLANs_and_VDOMs_Guide.pdf (viewed June 25, 2013).

62 http://www.techopedia.com/definition/25115/data-loss-prevention-dlp (viewed June 21, 2013).

63 http://www.techopedia.com/definition/5416/anti-virus-software (viewed June 21, 2013).

64 http://www.pcmag.com/encyclopedia/term/37816/anti-spam (viewed June 21, 2013).

65 http://www.issa-sac.org/info_resources/ISSA_20050421_Aventail_End_Point_Control.pdf (viewed June 26, 2013).

66 http://www.techopedia.com/definition/5107/wireless-local-area-network-wlan (viewed July 1, 2013).

67 FORT-NPS 000025-31, at 29.

wishes to interact with the firewall. I understand that the first benefit is referred to as application level data inspection, and that the latter benefit is referred to as transparency.[68] According to Dr. Keromytis, the ability to inspect data traffic at the application level enhances a UTM system's ability to implement virus inspection and DLP, and, although it would be possible to implement these functionalities without the patented technology, these functionalities would not be reliable and would be, in some instances, less effective, and in other instances, not effective at all.[69] According to Dr. Keromytis, transparency is beneficial in that it makes a network firewall easier to build and more efficient to deploy and manage.[70]

C. Patent-in-Suit

Issued on April 22, 1997, the '601 patent is entitled "Apparatus and Method for Providing a Secure Gateway for Communication and Data Exchanges between Networks."[71] I understand that the patent claims certain firewall technologies[72] that, among other things, allow application layer services to operate on a UTM system.[73]

D. Accused Products

The accused Fortinet products are UTM devices and include all products that contain the FortiOS operating system. All accused products are configurable to implement a transparent application layer IP

---

68 Conversation with Dr. Angelos Keromytis, June 7, 2013.

69 Conversation with Dr. Angelos Keromytis, June 7, 2013.

70 Conversation with Dr. Angelos Keromytis, June 7, 2013.

71 United States Patent Number 5,623,601, April 22, 1997. The Abstract of the '601 patent describes the invention: "An apparatus and method for providing a secure firewall between a private network and a public network are disclosed. The apparatus is a gateway station having an operating system that is modified to disable communications packet forwarding, and further modified to process any communications packet having network encapsulation address which matches the device address of the gateway station. The method includes enabling the gateway station to transparently initiate a first communications session with a client on a first network requesting a network service from a host on a second network, and a second independent communications session with the network host to which the client request was addressed. The data portion of communications packets from the first session are passed to the second session, and vice versa, by application level proxies which are passed the communications packets by the modified operating system. Data sensitivity screening is preferably performed on the data to ensure security. Only communications enabled by security administrator are permitted. The advantage is transparent firewall with application level security and data screening capability."

72 Complaint, at ¶ 12.

73 Conversation with Dr. Angelos Keromytis, June 7, 2013.

proxy server.[74] The accused products include the FortiGate, FortiWiFi, FortiGate Voice, FortiWiFi Voice, and FortiOne products.[75]

I understand that all systems running the FortiOS operating system are capable of being configured to run as a transparent application level proxy. For the purpose of my analysis, I have been instructed by Counsel to treat sales of all systems running the FortiOS as infringing.

It is my further understanding that several key UTM features, including antivirus, antispam, data loss prevention, and SSL-encrypted traffic inspection rely on application layer services when used in the accused products and, thus, the use of these features is enabled by the alleged infringement.[76]

It is my understanding that products containing FortiOS were first sold in May 2002,[77] and that NPS seeks damages beginning July 2004, six years prior to the July 6, 2010 filing of the original complaint in this dispute.[78]

1. FortiGate and FortiWifi Network Security Platform

The FortiGate appliances "offer a broad set of security and networking functions, including firewall, VPN, application control, antivirus, intrusion prevention, Web filtering, anti-spam and WAN acceleration."[79] All FortiGate and FortiWifi models run the FortiOS operating system[80] and feature Fortinet's application specific integrated circuit processors, marketed as FortiASIC processors.[81] Fortinet produces a wide range of FortiGate models that it classifies into desktop, mid-range, high-end, and virtual appliances.[82]

FortiGate desktop appliances with built-in capabilities to provide wireless access and secure

---

74 Plaintiff's Second Set of Interrogatories to Defendant Fortinet, Inc., April 5, 2011, at 6.
75 Fortinet, Inc.'s Supplemental Response to Plaintiff's Interrogatory No. 6, May 29, 2013.
76 Conversation with Dr. Angelos Keromytis, June 7, 2013.
77 http://www.fortinet.com/sites/default/files/basicfiles/FortinetBroch.pdf, (viewed June 20, 2013).
78 Plaintiff's Original Complaint for Patent Infringement, July 6, 2010.
79 FORT-NPS 148967-9079, at 8974.
80 FORT-NPS 148967-9079, at 8974.
81 FORT-NPS 148967-9079, at 8971.
82 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

wireless traffic are marketed as FortiWifi wireless security appliances.[83] FortiWifi appliances combine the FortiOS operating system and FortiASIC processors to provide UTM functions along with secure, wireless access, and networking capabilities.[84]

a. FortiGate Desktop Appliances

FortiGate desktop appliances consist of the FortiGate-20, 40, 60, and 80 product lines.[85] These products deliver FortiGate's network security products and technologies to small locations, remote offices, and customer premise equipment.[86] These appliances also come with WiFi as part of the FortiWifi line,[87] and the FortiGate-80 line of UTMs includes models with voice calling features, marketed at the FortiGate Voice and FortiWiFi Voice.[88] The individual product lines are distinguished by incremental improvements: increases in firewall throughput, types of threat protection, number of WAN interfaces, number of internal switch ports, number of power over Ethernet ports, management consoles, and PC card slots, among other features.[89]

b. FortiGate Mid-Range Appliances

FortiGate mid-range appliances consist of the FortiGate-100, 200, 600, 800, 1000, and 1240 product lines.[90] These products deliver FortiGate's network security products and technologies to small, medium, and large organizations, and their branches.[91] FortiGate's mid-range appliances are differentiated from their desktop appliances in that they provide the capabilities of the FortiGate Network

---

83 http://www.fortinet.com/products/fortiwifi/index.html (viewed June 24, 2013). *See also*, Bedwell Deposition, at 206-207.

84 http://www.fortinet.com/products/fortiwifi/index.html (viewed June 24, 2013).

85 http://www.fortinet.com/products/fortigate/index.html (viewed June 25, 2013).

86 http://www.fortinet.com/products/fortigate/index.html (viewed June 25, 2013).

87 http://www.fortinet.com/products/fortigate/index.html (viewed June 25, 2013).

88 http://www.fortinet.com/sites/default/files/productdatasheets/FGV80C_DS.pdf (viewed July 3, 2013); http://fortinet.globalgate.com.ar/pdfs/FortiGate/FWFV80CS_DS.pdf (viewed July 3, 2013).

89 http://www.fortinet.com/products/fortigate/20C.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/40C.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/60C-POE.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/60D.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/80C.html (viewed June 25, 2013).

90 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

91 *See e.g.*, http://www.fortinet.com/products/fortigate/100D.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/1240B.html (viewed June 25, 2013).

Security Platforms to larger scale organizations. The FortiGate-100D product is marketed for "small and medium business [and] branch offices of large enterprises," and the FortiGate-1240B product is marketed for "mid-size or large enterprise network[s]."[92] Variations among models within the mid-range product lines include a "rugged version," different management consoles, increases in firewall throughput, different feature sets, increased internal storage, number of power over Ethernet ports, IPv6-ready platforms, DC power options, ASIC acceleration, and increases in latency, among other features.[93]

c. FortiGate High-End Appliances

FortiGate high-end appliances consist of the FortiGate-3000 and 5000 product lines.[94] These products deliver NGFW security with high throughput, low latency, and multi-vector threat protection.[95] The FortiGate-3000 series products deliver Fortinet's Network Security Platforms to large enterprises and managed service providers.[96] The FortiGate-5000 series products deliver Fortinet's Network Security Platforms to high-speed service providers, data centers, and telecommunications networks.[97] The 5000 series is a chassis-based system with multiple security and networking blades that allow for scalability in the deployment of a FortiGate system.[98] The 5000 series also has many optional and customizable features that are sold by Fortinet to further improve and personalize the appliance.[99] These product lines are further distinguished by incremental improvements in the number of ports, firewall throughput, speed of FortiASIC processors, Gigabit Ethernet ports, scalability, latency, number IPS signatures, UTM

---

92 http://www.fortinet.com/products/fortigate/100D.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/1240B.html (viewed June 25, 2013).

93 http://www.fortinet.com/products/fortigate/rugged_100C.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/100D.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/200B.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/300C.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/600C.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/800C.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/1000C.html (viewed June 25, 2013);
http://www.fortinet.com/products/fortigate/1240B.html (viewed June 25, 2013).

94 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

95 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

96 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

97 http://www.fortinet.com/products/fortigate/index.html (viewed June 24, 2013).

98 http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-5101C.pdf (viewed June 25, 2013).

99 http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-5101C.pdf (viewed June 25, 2013).

features, NGFW features, and security blades, among other features.[100] Fortinet markets a subset of FortiGate-3000 series and 5000 series appliances as FortiCarrier appliances. In its annual report, Fortinet explains that it does so "to reflect products specifically targeting [a] subset of service providers. These products add incremental security networking and management functionality often utilized in service provider deployments."[101] According to its website, the FortiCarrier "platforms are designed to secure the business of mobile operators, voice operators, Managed Security Service Providers (MSSPs), and large enterprises, enabling the migration to next generation network architectures."[102]

d. FortiGate Virtual Appliances

FortiGate Virtual Appliances consist of the FortiGate-VM00, VM01, VM02, VM04, and VM08 product lines.[103] FortiGate virtual appliances are designed to work with physical appliances to provide network security within virtualized infrastructure environments.[104] They offer the same functionalities as physical appliances, but they are also able to "inspect inter-zone traffic between virtual machines and virtual network segments."[105] Patrick Bedwell, Vice President of Product Marketing at Fortinet, testified that the FortiGate virtual appliances are sometimes purchased together with the FortiGate physical appliances,[106] and Fortinet promotional materials state that the "[v]irtual appliances complement

---

100 http://www.fortinet.com/products/fortigate/3140B.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/3240C.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/3600C.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/3950series.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/5000series_blades.html (viewed June 25, 2013); http://www.fortinet.com/products/fortigate/5000series.html (viewed June 25, 2013).

101 FORT-NPS 148967-9079, at 974.

102 http://www.fortinet.com/sites/default/files/productdatasheets/FCRSeries_DS.pdf (viewed June 25, 2013).

103 http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-VM01.pdf (viewed June 24, 2013).

104 FORT-NPS 145605-13, at 09. A virtual machine ("VM") is "a tightly isolated software container with an operating system and application inside. Because each VM is completely separate and independent, many of them can run simultaneously on a single computer. A thin layer of software called a hypervisor decouples the VMs from the host, and dynamically allocates computing resources to each VM as needed." By allowing multiple "virtual machines" to operate on a single physical machine, virtualization more efficiently utilizes computing resources, reducing the need for redundant processors distributed across multiple physical appliances that are frequently underutilized. *See*, http://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works.html (viewed June 27, 2013); http://www.beyondvm.com/what-is-virtualization/ (viewed June 27, 2013).

105 FORT-NPS 145536-38, at 36-37.

106 Deposition of Patrick Bedwell, May 23, 2013 ("Bedwell Deposition"), at 47-49.

traditional Fortinet hardware appliances."[107] According to Mr. Bedwell, while FortiGate virtual appliances may be purchased with FortiGate physical appliances, the virtual appliances are not actually deployed on the physical appliance.[108] The individual product lines are distinguished by incremental improvements in firewall throughput, the maximum number of concurrent sessions on the firewall, IPS throughput, and antivirus throughput, amongst other features.[109]

e. FortiGate-One

FortiGate-ONE is a software product that is specifically designed to run the FortiOS operating system on the Hewlett-Packard ProCurve zl Blades for ProCurve 5400zl and 8200zl switches.[110] This product allows HP Networking customers to deploy "a single security blade with integrated firewall, antimalware, IPS, VPN, web filtering, antispam, application control, and data loss prevention."[111] According to Mr. Bedwell, FortiGate-ONE is no longer sold by Fortinet.[112]

2. FortiGate Voice and FortiWifi Voice

The FortiGate Voice and FortiWifi Voice models offer identical UTM, wireless access, and networking capabilities of similarly numbered FortiGate and FortiWifi appliance with the addition of secure voice over internet protocol ("VoIP") capabilities,[113] referred to as IP private branch exchanges ("PBX").[114] A PBX is a system that controls a company's phone lines and extensions.[115] The FortiGate Voice and FortiWifi Voice allow consolidation of all of the user's voice traffic into a single platform.[116] The different FortiGate Voice and FortiWifi Voice appliances offer UTM, networking, and wireless access and security capabilities similar to comparably numbered FortiGate and FortiWifi appliances.[117]

---

107 *See, e.g.*, FORT-NPS 000068-74, at 70; FORT-NPS 018399-405, at 401; FORT-NPS 018406-12, at 08.
108 Bedwell Deposition, at 215.
109 http://www.fortinet.com/products/fortigate/virtualappliances.html (viewed June 25, 2013).
110 FORT-NPS 017646-49, at 46.
111 http://h17007.www1.hp.com/one/alliance/fortinet/fortigate.htm (viewed June 25, 2009).
112 Bedwell Deposition, at 207.
113 Bedwell Deposition, at 207-208.
114 http://www.voip-info.org/wiki/view/PBX+System (viewed June 24, 2013).
115 http://www.voip-info.org/wiki/view/PBX+System (viewed June 24, 2013).
116 FORT-NPS 000077-78, at 78.
117 FORT-NPS 148967-079, at 974.

E. Other Fortinet Products

1. Products Used Exclusively with Accused Products

Fortinet markets several other products that are not accused in this matter, and I understand that several of these products are used together with accused FortiGate products.

FortiAP Wireless Access Points extend FortiGate security functions to wireless networks,[118] and I understand that they are designed for use exclusively with the accused FortiGate products.[119] I understand that FortiAP products do not contain the same operating system as that used in FortiGate products.[120]

Fortinet markets two types of security management products, the FortiManager and FortiAnalyzer, that are "[b]uilt to support FortiGate®, Wireless Security appliances FortiWiFi™ and other FortiOS™-enabled systems."[121] FortiManager products allow central management of multiple FortiOS-enabled appliances,[122] and FortiAnalyzer products aggregate and report on threats, inefficiencies and usage in FortiOS-enabled appliances.[123]

In addition, Fortinet markets accessories referred to as FortiModules that offer increased flexibility and performance for FortiGate and FortiCarrier platforms.[124] FortiModule products include accelerated interface modules that "deliver incremental firewall and IPsec VPN performance" to certain FG-300, 3000, and 5000 series appliances;[125] rear transition modules that "provide 10-Gigabit Ethernet backplane fabric connectivity" to FG-5000 series security blades;[126] Fortinet Mezzanine Card modules that add "10-Gigabit Ethernet and Gigabit (GbE) Ethernet interface options" and accelerated appliance security functions to FG-3950 series models;[127] security processing modules that enhance IPS, firewall

---

118 http://www.fortinet.com/products/fortiap/index.html (viewed June 24, 2013).
119 http://www.fortinet.com/wireless/Fortinet_WiFi_Sol_Guide.pdf (viewed June 24, 2013).
120 Deposition of Todd Nelson, June 26, 2013, ("Nelson Deposition"), at 131.
121 http://www.fortinet.com/solutions/network-security-management.html (viewed June 24, 2013).
122 http://www.fortinet.com/products/fortimanager/index.html (viewed June 24, 2013).
123 http://www.fortinet.com/products/fortianalyzer/index.html (viewed June 24, 2013).
124 http://www.fortinet.com/products/modules/index.html (viewed June 24, 2013).
125 http://www.fortinet.com/products/modules/accelerated_interface_modules.html (viewed June 26, 2013).
126 http://www.fortinet.com/products/modules/rear_transition_modules.html (viewed June 26, 2013).
127 http://www.fortinet.com/products/modules/fmc_modules.html (viewed June 26, 2013).

and IP multicast capabilities for certain FG-1000, 3000 and 5000 series models;[128] bypass modules that provide bypass functionality to certain FG-300, 600, 1000, 3000, and 5000 series models;[129] and storage modules that expand local storage "to enable security and system event logging, WAN optimization, and local web caching functions" in certain FG-300, 600, 3000 and 5000 models.[130]

2. Products That Have Increased Functionality When Used with Accused Products

The FortiSwitch l and the FortiToken product lines, may be used without FortiOS-enabled products, but both product families offer enhanced capabilities when used together with the accused products.[131] FortiSwitch products help to create secure access to Ethernet switches and allow for the scaling of network infrastructure.[132] FortiToken strong authentication products provide security by enabling two-factor authentication that reduces the risk of compromise relative to single-factor authentication.[133]

3. Products That May Be Used without Accused Products

Fortinet also markets several products that may be used with or without the Fortinet network security appliances that run the FortiOS operating system.

Fortinet markets web application firewalls under the trade name FortiWeb. These appliances protect web-based applications and internet-facing data.[134] A diagram on a FortiWeb product sheet indicates that FortiWeb appliances may be deployed with FortiGate devices, and its deployment options include a "True Transparent Proxy" option, which it describes as a "[l]ayer two deployment with no need for network level redesign."[135] The FortiWeb appliance does not run the FortiOS operating system.[136]

---

128 http://www.fortinet.com/products/modules/security_processing_modules.html (viewed June 26, 2013).
129 http://www.fortinet.com/products/modules/bypass.html (viewed June 26, 2013).
130 http://www.fortinet.com/products/modules/storage_module.html (viewed June 26, 2013).
131 http://www.fortinet.com/sites/default/files/productdatasheets/FortiSwitch-348B.pdf (viewed June 24, 2013).
132 http://www.fortinet.com/products/fortiswitch/index.html (viewed June 24, 2013); http://www.fortinet.com/sites/default/files/productdatasheets/FortiSwitch-348B.pdf (viewed June 24, 2013).
133 http://www.fortinet.com/products/fortitoken/index.html (viewed June 24, 2013); http://www.fortinet.com/sites/default/files/productdatasheets/FortiToken-300.pdf (viewed June 24, 2013); http://www.fortinet.com/products/fortitoken/200CD.html (viewed June 24, 2013);.
134 http://www.fortinet.com/products/fortiweb/index.html (viewed June 24, 2013).
135 http://www.fortinet.com/sites/default/files/productdatasheets/FortiWeb-4000D.pdf (viewed June 24, 2013).

FortiMail is an email security platform that provides antispam, antivirus, antiphishing, antimalware, data leakage prevention, identity based encryption, message archival and antiblacklisting services.[137] FortiMail products do not operate the FortiOS operating system,[138] and, while they can operate as stand-alone devices, they may also be integrated with FortiOS-enabled appliances.[139]

Additional products that appear to be able to operate independent of FortiOS-enabled appliances include FortiScan,[140] FortiDB,[141] FortiBridge,[142] FortiBalancer,[143] FortiCache,[144] FortiAuthenticator,[145] FortiDNS,[146] FortiClient,[147] FortiVoice,[148] FortiDDoS,[149] and FortiCamera.[150]

F. Economic Footprint of the Patent-at-Issue

From the perspective of assessing damages associated with the alleged infringement of the patent-at-issue, an important consideration is the "economic footprint" of the patent. This refers to the manner in which the incorporation of the specific technologies covered by the patent-at-issue into the accused

---

136 Nelson Deposition, at 132.

137 http://www.fortinet.com/products/fortimail/index.html (viewed June 24, 2013).

138 Nelson Deposition, at 132.

139 http://www.fortinet.com/products/fortimail/5002B.html (viewed June 24, 2013).

140 FortiScan products monitor and scan endpoints for security and provide auditing and compliance evaluations. *See*, http://www.fortinet.com/products/fortiscan/index.html (viewed June 24, 2013).

141 FortiDB software provides a database security platform that also helps meet compliance requirements. *See*, http://www.fortinet.com/products/fortidb/index.html (viewed June 24, 2013).

142 FortiBridge bypass appliances help to ensure network continuity by providing new routes for network traffic in the event of system or power failure. *See*, http://www.fortinet.com/products/fortibridge/index.html (viewed June 24, 2013).

143 FortiBalancer products balance server loads by distributing application load over multiple servers. *See*, http://www.fortinet.com/products/fortibalancer/index.html (viewed June 24, 2013).

144 FortiCache products address bandwidth saturation, high latency, and poor performance through the caching of popular internet content. *See*, http://www.fortinet.com/products/forticache/index.html (viewed June 24, 2013).

145 FortiAuthenticator products allow for increased security by enabling authentication for a network. *See*, http://www.fortinet.com/products/fortiauthenticator/index.html (viewed June 24, 2013).

146 FortiDNS products provide a caching domain name system (DNS) with a focus on security. *See*, http://www.fortinet.com/products/fortidns/1000C.html (viewed June 24, 2013).

147 FortiClient software extends FortiGate's UTM to endpoints on a network (like desktops, laptops, tablets, and smartphones). FortiClient can also be downloaded as standalone protection, meaning that it does not need to be associated with a FortiGate secured network. *See*, http://www.fortinet.com/products/endpoint/index.html (viewed June 24, 2013).

148 FortiVoice products are phones and phone systems meant for business telephone communications. *See*, http://www.fortinet.com/products/fortivoice/index.html (viewed June 24, 2013).

149 FortiDDos products provide detection and prevention of Distributed Denial of Service ("DDoS") attacks. *See*, http://www.fortinet.com/products/fortiddos/index.html (viewed June 24, 2013).

150 FortiCamera products are cameras that are meant for video surveillance and security. *See*, http://www.fortinet.com/products/forticamera/index.html (viewed June 24, 2013).

products contributes to the quality and features of these products and, ultimately, to consumers' willingness and desire to purchase them.

Demand for Fortinet products is influenced both directly and indirectly by the technology enabled by the '601 patent. The technology of the '601 patent directly influences demand to the extent that customers value the enhanced data security an application layer IP proxy server offers relative to other options.

The '601 patent indirectly influences demand to the extent that purchasing decisions are influenced by UTM features that are associated with an infringing transparent application layer configuration. These features include antivirus, antispam, DLP, and SSL-encrypted traffic inspection.[151] In other words, it is my understanding that, but for the '601 patent, none of these features would be able to operate on systems running FortiOS in a manner that would be acceptable to customers.[152]

1. Direct Demand for the '601 Technology

The link between the patented technology and demand for Fortinet products is evident from deposition testimony, third party reviews of FortiGate products, customer feedback, and Fortinet's marketing materials, each of which emphasize the infringing functionality.

According to Michael Xie, Chief Technology Officer and Vice President of Engineering at Fortinet,[153] the ability to run application-layer processes was an important driver of demand for FortiGate UTMs. Mr. Xie testified that it was "very important" to the functionality of a UTM firewall and if those features did not run "the user wouldn't get what they want."[154] Additionally, Mr. Xie testified that the majority of customers that purchased FortiGate UTMs would use at least one of the application processes running on the FortiGate system, and, furthermore, he asserted that without these processes, customers would not want to purchase FortiGate UTMs.[155]

---

151 Conversation with Dr. Angelos Keromytis, June 7, 2013.
152 *See, e.g.*, Deposition of Michael Xie, June 27, 2013, rough transcript ("Xie Deposition"), at 95-96.
153 http://www.fortinet.com/aboutus/management.html (viewed June 30, 2013)
154 Xie Deposition, at 95-96.
155 Xie Deposition, at 97-98.

A 2004 market assessment by IDC reported that "Fortinet believes that its technology is the only platform that can deliver application-layer services (*e.g.*, virus detection and content filtering) at real-time multigigabit/second data rates,"[156] and in 2012 Frost & Sullivan stated that "Fortinet appliances provide protection from both network-layer and application-layer attacks."[157] Another analyst report from 2010 observed that the introduction of new FortiGate models had expanded Fortinet's application-layer security features.[158]

According to Mr. Bedwell, Fortinet marketed its products through press releases, white papers, data sheets, competitive analyses, and sales presentations.[159] These marketing materials routinely mentioned application layer services. For example, one product sheet discussed FortiGate Application Proxy Firewalls, noting that "Proxy firewalls provide the advantage of restricting information flows at the application level and the benefit of better security" and stating that the "integrated hardware and software architecture [was] specifically designed for high-performance, application-level content processing."[160] This information sheet claimed that "FortiGates are the only application-level firewalls that meet the current CCEVS criteria."[161] A sales presentation for the FortiGate-50 and FortiGate-100 series appliances claims that they "[u]tilize purpose-built platforms that effectively block todays application- and network-borne attacks."[162]

Fortinet press releases also mentioned the importance of application layer services. A 2003 press release indicated that Gartner had classified Fortinet as a "Visionary" after changing its rating criteria to "reflect a new emphasis on application-layer capabilities."[163] The press release further claimed that "FortiGate Antivirus Firewalls are based on a groundbreaking architecture designed specifically to deliver application-layer security and content processing services in addition to network-layer services in real

---

156 FORT-NPS 061580-88, at 84.
157 FORT-NPS 146229-36, at 33.
158 FORT-NPS 145513-14, at 13.
159 Bedwell Deposition, at 18-19, 136.
160 FORT-NPS 019002-03.
161 FORT-NPS 019002-03, at 03.
162 FORT-NPS 019321-51, at 23.
163 FORT-NPS 064422-24, at 23.

time."[164] In a press release announcing an endorsement from Miercom, an independent networking consultancy and product test center, James Lie, director of product management at Fortinet at the time, stated that "[b]y integrating and enhancing the performance both of network-layer and application-layer functions, the FortiGate platforms represent a major stop in the continuing evolution of network protection…This endorsement from Miercom validates our approach and assures our customers that Fortinet delivers world-class network security."[165] In another press release, a FortiGate reseller said that the fact that FortiGate "delivers its high performance and multi-zone abilities not just for firewall and VPN but also for application-layer services like antivirus in nothing short of miraculous."[166]

One Fortinet customer pointed to the application-layer services as a consideration in deciding to purchase a FortiGate system. Rick Huang, director of IT services at AltiGen stated that "[b]y implementing Fortinet's FortiGate system with their application-layer architecture and VoIP-aware features AltiGen is able to support the full range of IP telephony needs of our remote employees without compromising security."[167]

Fortinet White Papers also pointed to application layer services as notable attributes of FortiGate UTMs. A July 2007 white paper reported that "Fortinet's integration of application-layer and network layer functionality" offers improved security over older security solutions,[168] and a 2009 Solution Guide concluded that "Enterprises need additional layers of protection" to protect against application layer threats;[169]

2. Indirect Demand for the '601 Technology

Evidence from deposition testimony of Fortinet personnel, third parties, and Fortinet's own marketing materials also indicates that the antivirus, antispam, DLP, and SSL-encrypted traffic inspection functions, whose use is associated with infringing configurations of the accused products, all influence

164 FORT-NPS 064422-24, at 23. *See also*, FORT-NPS 064346-48, at 47.
165 FORT-NPS 064312-13.
166 FORT-NPS 064317-19, at 19.
167 FORT-NPS 064392-94, at 92.
168 FORT-NPS 017383-92, at 90.
169 FORT-NPS 019179-86, at 86.

demand for the accused products. As each of these functionalities is associated with an infringing transparent application level proxy configuration, evidence that these attributes drive demand is evidence of the indirect effect of the '601 patent on demand for the infringing products.

In his deposition, Mr. Bedwell stated that it was his belief that customers demand these features:

> [S]ome of the additional technologies are extremely important for customers such as application control; intrusion prevention; threat protection; say, antivirus; web content filtering… all those features that we have in our FortiGate, some customers buy our FortiGates because of that -- one or more of those features, so potentially any one of those can be the reason they bought our FortiGate versus somebody else's.[170]

Third-party sources cite Fortinet's integration of several of these features as reasons for Fortinet's success in the marketplace. A FortiGate-3600 product review by CRN noted that it included elements such as firewall, antivirus, VPN, IPS, content filtering, and traffic management that were "vital to network security."[171] I understand that, among the elements listed by CRN, antivirus and content filtering are associated with infringing configurations of accused products.[172] A 2012 Frost & Sullivan report indicated that "Fortinet offers a strong value proposition of comprehensive network security in a single, easily deployed network appliance… FortiOS is the operating system that powers all of the FortiGate® security products and each FortiGate device includes the full suite of security technologies" including antispam and DLP, among other features.[173] A 2010 Frost & Sullivan review of the global UTM market described Fortinet as the market leader in the UTM market and stated that its market strategy was to offer "a broad suite of security technologies, such as firewall, VPN, IPS, antimalware, antispam, and Web content filtering, that when combined, constitute a comprehensive threat management solution."[174] In a 2011 publication, Frost & Sullivan reported that one customer, American Axle & Manufacturing ("AAM"), chose Fortinet's integrated security platform because of the "flexibility and feature-rich

---

170 Bedwell Deposition, at 115.
171 FORT-NPS 064133-35, at 33.
172 Conversation with Dr. Angelos Keromytis, June 7, 2013.
173 FORT-NPS 146991-97, at 93.
174 FORT-NPS 146680-774, at 752, 753.

capabilities its UTM appliances are able to offer."[175] In particular, features that were highly valuable to AAM included one of the capabilities associated with infringement, DLP, along with other features such as content filtering, WAN optimization, and VPN.[176] A January 2013 Current Analysis report identified the combination of multiple security features, including antivirus, DLP, and antispam, as one of Fortinet's strengths,[177] and a November 2010 Current Analysis report noted that DLP and SSL inspection were two of the "four major new capabilities" that were added to Fortinet's FortiOS 4.0 upgrade "along with hundreds of other improvements."[178]

Recent Fortinet press releases also mention many of the features associated with infringement. A June 2013 press release touted the ability to easily configure FortiGate appliances for many features including DLP.[179] A May 2013 press release stated that a customer intended to use Fortinet products, including the FortiGate platform, to provide security features including firewall, IPS, DLP, application control, antivirus, URL filtering, and secure Wi-Fi.[180]

Fortinet marketing materials also consistently highlight the capabilities associated with the alleged infringement. A recent Fortinet White Paper discussed the importance of protection against viruses and other forms of web-based intrusion and noted that the "solution must also be easy to configure, deploy and manage;"[181] another White Paper noted that anti-virus and anti-spam are both security modules that occur in the application layer;[182] a 2011 White Paper included antivirus, antispam, DLP, and traffic inspection as key elements in the next generation of security platforms;[183] and a 2012 White Paper promoted FortiGate as an ideal application for online retailers because it delivers "the broadest range of network services on the market, including: firewall, VPN, traffic shaping, IPS,

175 FORT-NPS 146779-82, at 80.
176 FORT-NPS 146779-82, at 80.
177 FORT-NPS 145497-501, at 497.
178 FORT-NPS 145503-12, at 04.
179 http://www.fortinet.com/press_releases/2013/new-enterprise-firewall-advances-fortinet-network-security-platform.html (viewed on June 19, 2013).
180 http://www.fortinet.com/press_releases/2013/Fortinet-Expands-FishNet-Security-Relationship.html (viewed on June 19, 2013).
181 FORT-NPS 143528-44, at 43.
182 FORT-NPS 019239-64, at 52.
183 FORT-NPS 151244-63, at 46, 52, 54, 57, 60.

antimalware, application control, [DLP], vulnerability management and many more security functions.[184] In addition to these White Papers, many recent product reviews and Fortinet sales presentations and data sheets also mention antivirus,[185] antispam,[186] DLP,[187] and SSL-encrypted traffic inspection[188] capabilities of FortiGate products. Fortinet competitive analyses also emphasize several of these features. Competitive analyses comparing Fortinet UTMs to WatchGuard and SonicWALL UTMs compared several features including anti-virus, IPS, SSL content inspection, and anti-spam.[189]

3. Other Drivers of Demand

Product attributes enabled by the patented technology are not the only drivers of demand for the accused products. As noted above, one customer, AAM, considered content filtering, WAN optimization, and VPN to be important factors in its decision to purchase a FortiGate product.[190] A CRN product review included content filtering and traffic management among the critical elements of network security provided by the FortiGate-3600; this review also pointed to the FortiGate's "ASIC-based design and redundant power supplies" as attributes that contribute to FortiGate performance.[191] Several market analysts have indicated that Fortinet's ASIC technology is a factor that many customers consider.[192] Frost & Sullivan awarded Fortinet with its "2008 Global Market Leadership Award" and reported that it believed that the "unique ASIC technology makes [Fortinet] the prominent leader in the UTM market.[193] Third parties also have identified features such as VPN, application control, and web content filtering,

---

184 FORT-NPS 143604-08, at 06.

185 For examples of product reviews, *see* FORT-NPS 060512-13; FORT-NPS 061740-41. For examples of sales presentations, *see* FORT-NPS 017417-54; FORT-NPS 017834-53; FORT-NPS 017938-52. For examples of data sheets, *see* FORT-NPS 000003-09; FORT-NPS 000025-31; FORT-NPS 000050-53.

186 For examples of product reviews, *see* FORT-NPS 061740-41. For examples of sales presentations, *see* FORT-NPS 017417-54; FORT-NPS 019476-516; FORT-NPS 019593-636. For examples of data sheets, *see* FORT-NPS 000025-31; FORT-NPS 000050-53; FORT-NPS 017809-14.

187 For examples of sales presentations, *see* FORT-NPS 019476-516; FORT-NPS 019593-636; FORT-NPS 017938-52. For examples of product data sheets, *see* FORT-NPS 000025-31; FORT-NPS 000050-53; FORT-NPS 017809-14.

188 For examples of sales presentations, *see* FORT-NPS 017834-53. For examples of product data sheets, *see* FORT-NPS 000025-31; FORT-NPS 017809-14; FORT-NPS 000003-09.

189 Bedwell Exhibit 61, at 2; Bedwell Exhibit 62, at 2.

190 FORT-NPS 146779-82, at 80.

191 FORT-NPS 064133-35, at 33.

192 *See, e.g.*, FORT-NPS 145497-502, at 498; FORT-NPS 146413-47, at 17; FORT-NPS 145513-14, at 13.

193 FORT-NPS 146192-94, at 93.

among other things, as important features of Fortinet products.[194] Fortinet data sheets identify these and many other features in their descriptions of FortiGate capabilities.[195] For example, a data sheet describing the FortiGate-5000 series of UTMs describes them as "carrier-class hardware components with advanced FortiASIC™ acceleration, a modular architecture, and multi-threat security from the FortiOS™ operating system," and notes that the FortiOS software enables several features, including VPN, web filtering, application control, vulnerability management, and end point network access control.[196]

FortiGate products also include several physical hardware characteristics that influence demand for the accused products. FortiWifi products include wireless transmitters that provide secure wireless access;[197] and FortiGate Voice and FortiWifi Voice products add VoIP capabilities to FortiGate and FortiWifi appliances. These capabilities are promoted by Fortinet,[198] and I understand that secure wireless and VoIP capabilities do not infringe the '601 patent when deployed on Fortinet appliances running the FortiOS operating system.

4. Summary

Taken together, the evidence that I have reviewed suggests that the patent-in-suit either directly or indirectly drives demand for products running the FortiOS operating system. Although the patent-in-suit is not the sole demand driver, it is directed to more than a "trivial" feature; rather, it contributes substantially to demand for the accused products.[199]

III. DAMAGES FRAMEWORK

Recovery for patent infringement is governed by 35 U.S.C. § 284, which provides:

> Upon finding for the claimant the court shall award the claimant damages adequate to compensate for the infringement, but in no event

---

194 *See, e.g.*, FORT-NPS 146991-97, at 93; FORT-NPS 146680-774, at 753; FORT-NPS 146935-39, at 38; FORT-NPS 145497-502, at 497.

195 *See, e.g.*, FORT-NPS 018497-502; FORT-NPS 017523-26; FORT-NPS 017545-48; FORT-NPS 017519-22; FORT-NPS 017531-34.

196 FORT-NPS 018497-502, at 497.

197 *See, e.g.*, FORT-NPS 019529-40, at 37-38.

198 *See, e.g.*, FORT-NPS 019529-40, at 37-38; FORT-NPS 000003-09, at 08; FORT-NPS 000014-20, at 19; FORT-NPS 000066-67; FORT-NPS 000077-78.

199 *See, e.g.*, *Uniloc USA, Inc. v. Microsoft Corporation*, 632 F. 3d 1292, 1318 (Fed. Cir. 2011).

> less than a reasonable royalty for the use made of the invention by the infringer.

This provision has been interpreted to mean that the holder of an infringed patent should be placed in the same financial position it would have been in had its patent not been infringed.[200] If infringement is found, the patent holder is entitled to receive as damages the value of the asset that was taken.[201] In *Aro Manufacturing*, the U.S. Supreme Court wrote that the statutory measure of "damages" is "the difference between [the patent owner's] pecuniary condition after the infringement, and what his condition would have been if the infringement had not occurred."[202]

The two most common forms of damages in patent infringement cases are lost profits and a reasonable royalty. It is my understanding that NPS does not seek lost profits in this dispute and is seeking damages in the form of a reasonable royalty. A reasonable royalty represents the payment or stream of payments that the alleged infringer should have paid for use of the patent holder's technology.

IV. REASONABLE ROYALTY DAMAGES

As noted above, a patent holder who is able to establish liability for patent infringement is entitled to no less than "a reasonable royalty for the use made of the invention by the infringer."[203] Reasonable royalty damages are, therefore, the statutory minimum, or, as described by the Court of Appeals for the Federal Circuit ("Federal Circuit"), "the floor below which damages shall not fall."[204]

A. Legal Framework

As I understand it, courts are generally afforded some degree of discretion and latitude in making reasonable royalty determinations, and fact-finders have relied upon a range of approaches and evidence

---

200 *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 507 (1964); *Lucent Techs. Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009).

201 *See, Trell v. Marlee Electronics Corp.*, 912 F.2d 1443, 1446-47 (Fed. Cir. 1990) (indicating that the measure of damages in a patent case is the value of "that which the defendant has appropriated"). *See also, Dowagiac Mfg. Co. v. Minnesota Moline Plow Co.*, 235 U.S. 641, 648 (1915) ("[T]he normal measure of damages is the value of what was taken."); *Faulkner v. Gibbs*, 199 F.2d 635, 638 (9th Cir. 1952) (Damages are "measured ordinarily by the fair value of what was taken, *i.e.*, the privilege of making, using or selling the patented article.").

202 *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U.S. 476, 507 (1964).

203 35 U.S.C. § 284.

204 *Bandag, Inc. v. Gerrard Tire Co.*, 704 F.2d 1578, 1583 (Fed. Cir. 1983).

in making such determinations.[205] As explained by the court in *Georgia-Pacific*:[206]

> [T]here is a multiplicity of inter-penetrating factors bearing upon the amount of a reasonable royalty. But *there is no formula* by which these factors can be rated precisely in the order of their relative importance or by which their economic significance can be automatically transduced into their pecuniary equivalent. In discharging its responsibility as fact finder, the Court has attempted to exercise a discriminating judgment reflecting its ultimate *appraisal of all pertinent factors* in the context of the credible evidence.

Since its issuance, the *Georgia-Pacific* decision has become "the touchstone of modern reasonable royalty analysis"[207] and "established principles that have been used by virtually every court since in determining a reasonable royalty."[208] The court in *Georgia-Pacific* identified a non-exhaustive list of factors that may be relevant for the determination of a reasonable royalty in a patent infringement case. These factors are:

1. The royalties received by the patentee for the licensing of the patent in suit, proving or tending to prove an established royalty.

2. The rates paid by the licensee for the use of other patents comparable to the patent in suit.

3. The nature and scope of the license, as exclusive or non-exclusive; or as restricted or non-restricted in terms of territory or with respect to whom the manufactured product may be sold.

4. The licensor's established policy and marketing program to maintain his patent monopoly by not licensing others to use the invention or by granting licenses under special conditions designed to preserve that monopoly.

5. The commercial relationship between the licensor and licensee, such as, whether they are competitors in the same territory in the same line of business; or whether they are inventor and promoter.

6. The effect of selling the patented specialty in promoting sales of other products of the licensee; the existing value of the invention to the licensor as a generator of sales of his non-patented items; and the extent of such derivative or convoyed sales.

7. The duration of the patent and the term of the license.

---

[205] *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120-21 (S.D.N.Y. 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971).

[206] *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120-21 (S.D.N.Y. 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971) (emphasis added).

[207] Richard F. Cauley, *Winning the Patent Damages Case*, Oxford University Press (2009), at 7.

[208] Richard F. Cauley, *Winning the Patent Damages Case*, Oxford University Press (2009), at 12.

8. The established profitability of the product made under the patent; its commercial success; and its current popularity.

9. The utility and advantages of the patent property over the old modes or devices, if any, that had been used for working out similar results.

10. The nature of the patented invention; the character of the commercial embodiment of it as owned and produced by the licensor; and the benefits to those who have used the invention.

11. The extent to which the infringer has made use of the invention; and any evidence probative of the value of that use.

12. The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the invention or analogous inventions.

13. The portion of the realizable profit that should be credited to the invention as distinguished from non-patented elements, the manufacturing process, business risks, or significant features or improvements added by the infringer.

14. The opinion testimony of qualified experts.

15. The amount that a licensor (such as the patentee) and a licensee (such as the infringer) would have agreed upon (at the time the infringement began) if both had been reasonably and voluntarily trying to reach an agreement; that is, the amount which a prudent licensee – who desired, as a business proposition, to obtain a license to manufacture and sell a particular article embodying the patented invention – would have been willing to pay as a royalty and yet be able to make a reasonable profit and which amount would have been acceptable by a prudent patentee who was willing to grant a license.[209]

In addition to these factors (which are often referred to as "*Georgia-Pacific* factors"), courts have articulated a number of other principles to consider in the determination of a reasonable royalty in a patent infringement proceeding.

As noted above, the Supreme Court in *Aro Manufacturing Co.* described an appropriate damages award, of which a reasonable royalty is one form, as "compensation for the pecuniary loss … [the patentee] has suffered from the infringement, without regard to the question whether the defendant has gained or lost by his unlawful acts."[210] The Federal Circuit has added that "the purpose of compensatory

[209] *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971).

[210] *Aro Mfg. Co., Inc. v. Convertible Top Replacement Co.*, 377 U.S. 476, 507 (1964) (citing *Coupe v. Royer*, 155 U.S. 565, 582). *See also, ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 869 (Fed. Cir. 2010) ("At all times,

damages is not to punish the infringer, but to make the patentee whole."[211] With regard to the scope of coverage of a reasonable royalty, the Federal Circuit has emphasized that "the trial court must carefully tie proof of damages to the claimed invention's footprint in the market place."[212]

B. Hypothetical Negotiation Construct

1. Overview

One of the most common tools used in reasonable royalty analyses is the "hypothetical negotiation" construct, which frames the analysis using a hypothetical arm's-length negotiation for a license to practice the patent(s)-at-issue between a willing patent owner and a willing potential licensee at the point of first alleged infringement.[213] This construct is reflected in *Georgia-Pacific* Factor 15. In applying the hypothetical negotiation construct in the analysis of reasonable royalty damages, it is assumed that the negotiation is conducted using several assumptions:

1. the patent is known to be valid and enforceable at the time infringement commences;
2. the patent is known to be infringed;
3. the patent holder is willing to issue a license;
4. the licensee is willing to take a license; and
5. the appropriate relevant business facts (even subsequent to the point of negotiation) are deemed known to both parties.[214]

---

the damages inquiry must concentrate on compensation for the economic harm caused by infringement of the claimed invention.").

211 *Pall Corp. v. Micron Separations, Inc.*, 66 F.3d 1211, 1223 (Fed. Cir. 1995).

212 *ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 869 (Fed. Cir. 2010).

213 *See, Riles v. Shell Exploration and Production Co.*, 298 F.3d 1302, 1311 (Fed. Cir. 2002) ("A 'reasonable royalty' contemplates a hypothetical negotiation between the patentee and the infringer at a time before the infringement began."). *See also, Hanson v. Alpine Valley Ski Area, Inc.*, 718 F.2d 1075, 1078 (Fed. Cir. 1983); *Lucent Technologies, Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1325 (Fed. Cir. 2009) ("The hypothetical negotiation tries, as best as possible, to recreate the *ex-ante* licensing negotiation scenario and to describe the resulting agreement. In other words, if infringement had not occurred, willing parties would have executed a license agreement specifying a certain royalty payment scheme. The hypothetical negotiation also assumes that the asserted patent claims are valid and infringed."). In *Lucent*, the Federal Circuit suggested that the hypothetical negotiation construct was an alternative to "the analytical method" (which focuses on the allocation of an infringer's profits attributable to the accused products) in the assessment of reasonable royalty damages. *See, Lucent v. Gateway*, 580 F.3d 1301, 1324-25 (Fed. Cir. 2009). In this report, information derived from the various valuation methodologies, including the analytical method, is used in the context of the hypothetical negotiation construct to determine a reasonable royalty.

214 *See*, Paul M. Janicke, *Contemporary Issues in Patent Damages*, 42 AM. UNIV. L.R. 691, 722-24 (Spring 1993). *See also, Innogenetics, N.V. v. Abbott Labs.*, 578 F. Supp. 2d 1079, 1093-94 (W.D. Wis. 2007) ("In

Although the hypothetical negotiation construct is a useful tool for analyzing a reasonable royalty, courts have cautioned that a negotiation conducted after infringement has occurred (and been proven) is not the same as a negotiation between truly willing parties prior to the date of first infringement.[215] As explained by the Court in *Panduit*:

> The setting of a reasonable royalty after infringement cannot be treated … as the equivalent of ordinary royalty negotiations among truly "willing" patent owners and licensees. That view would constitute a pretense that the infringement never happened. It would also make an election to infringe a handy means for competitors to impose a "compulsory license" policy upon every patent owner. … As said by this court in another context, the infringer would be in a "heads-I-win, tails-you-lose" position.[216]

In other words, in applying the hypothetical negotiation construct, one must be mindful not to under-compensate the patent holder for the alleged infringement and, thereby, create incentives for a potential infringer to use infringement as a means of obtaining an advantageous compulsory license.

At the same time, the fact that the hypothetical negotiation is assumed to take place at the point of first infringement (*i.e.*, after the alleged infringer has committed resources to the allegedly infringing activity) creates a risk that the patent holder would be able to extract concessions in a hypothetical negotiation that exceed the actual contribution made by the allegedly infringed patent to the value of the allegedly infringing product. As noted above, I understand that reasonable royalty damages should not include amounts beyond that which was contributed by the patent at issue.

---

calculating the amount of a reasonable royalty, the jury has to pretend that the parties sat down and negotiated a reasonable royalty before the day that defendant began its infringement of the plaintiff's patent. Unlike a real negotiation, this hypothetical negotiation assumes that the infringer must agree to some amount of royalty payment; it does not have the option of walking away from the table. The jury must put itself in the shoes of the parties and look at the relevant circumstances as they were at the time the negotiations would have taken place. The reasonable royalty calculus assesses the relevant market as it would have developed before and absent the infringing activity." (*Internal citations omitted*)).

[215] *See, e.g., Panduit Corp. v. Stahlin Bros. Fibre Works*, 575 F.2d 1152 (6th Cir. 1978); *Stickle v. Heublein, Inc.*, 716 F.2d 1550 (Fed. Cir. 1983).

[216] *Panduit Corp. v. Stahlin Bros. Fibre Works*, 575 F.2d 1152, 1158 (6th Cir. 1978) (citation omitted).

Given these challenges associated with the application of the hypothetical negotiation construct, the Federal Circuit has noted that "[t]he willing licensee/licensor approach must be flexibly applied as a 'device in the aid of justice.'"[217] One particular dimension of flexibility that is incorporated into the analysis of a hypothetical negotiation is consideration of the "book of wisdom,"[218] which includes "considering facts and circumstances that may have occurred after the time of infringement in determining what negotiators would have decided at that time."[219]

2. Date of Hypothetical Negotiation

According to the Federal Circuit, the date of a hypothetical negotiation is the date at which infringement of a valid and enforceable patent first occurred.[220] Typically, this has been interpreted to be the point of the first commercial sale of a product embodying an issued patent. This makes sound economic sense, as this is typically the first point at which both parties – the patent owner and the accused infringer – recognize the need for a license negotiation.

In this case, the issue date of the patent-in-suit is April 22, 1997.[221] The first commercial sale of a product containing a FortiOS occurred in May 2002.[222] Although NPS does not seek damages here prior to July 2004 (six years before the filing of the complaint on July 6, 2010),[223] the hypothetical negotiation occurs at the date of first infringing sale – May 2002.

3. Parties to the Negotiation

The parties to the hypothetical negotiation are the patent holder at the time of the first alleged infringement and the alleged infringer.

The '601 patent was filed and assigned to Milkyway Networks Corporation in November 1994,

---

217 *TWM Manufacturing Co. v. Dura Corp.*, 789 F.2d 895, 900 (Fed. Cir. 1986).

218 *Fromson v. Western Litho Plate and Supply Co.*, 853 F.2d 1568, 1575 (Fed. Cir. 1988) ("Experience is then available to correct uncertain prophecy. Here is a book of wisdom that courts may not neglect. We find no rule of law that sets a clasp upon its pages, and forbids us to look within.").

219 Bryan W. Butler, *Patent Infringement: Compensation and Damages*, Law Journal Press (2009), at §4.02.

220 *See, Wang Labs., Inc. v. Toshiba Corp.*, 993 F.2d 858 (Fed. Cir. 1993).

221 Complaint, at ¶ 10.

222 http://www.fortinet.com/sites/default/files/basicfiles/FortinetBroch.pdf (viewed June 25, 2013).

223 Complaint, at 6.

but it was not issued until April 22, 1997.[224] The '601 patent was acquired by SLM Networks Corporation ("SLM") in October 1998, and in February 2004 it was acquired by Bevertec CST, Inc. ("Bevertec").[225] In June 2006, Bevertec and Mount Hamilton Partners, LLC ("Mount Hamilton") entered into a patent agreement that transferred rights to Mount Hamilton in August 2006, but, as a part of this agreement, Bevertec retained a royalty-free non-exclusive worldwide right to practice the '601 patent.[226] NPS acquired rights to the patent-in-suit on April 30, 2010 when the rights the '601 patent were transferred from Mount Hamilton to NPS.[227] Thus, at the time of the hypothetical negotiation with Fortinet in May 2002, SLM was the patent holder.

SLM was a subsidiary of SLMSoft, Inc. ("SLMSoft"), an Ontario, Canada based company that declared bankruptcy in 2003.[228] SLMSoft "developed electronic payment systems and transaction processing solutions, including e-commerce applications, with a focus on the financial services industry."[229] I am not aware of information indicating either SLMSoft or its subsidiary, SLM, have ever been manufacturers or distributors of network security appliances. Thus, it appears that they have never competed with Fortinet for sales of such products.

C. Reasonable Royalty Analysis

1. Overview

To estimate a reasonable royalty, I typically employ a four-part analysis. First, I determine the appropriate form of a royalty-bearing license. Second, to the extent appropriate, I determine the appropriate royalty base – *i.e.*, the measure of allegedly infringing activity – to which a reasonable royalty

---

224 Plaintiff Network Protection Sciences, LLC's Objections and Responses to Defendant Fortinet, Inc.'s First Set of Interrogatories, March 1, 2013 ("NPS Response to First Set of Interrogatories"), at 6; U.S. Patent No. 5,623,601.

225 NPS Response to First Set of Interrogatories, at 6.

226 NPS Response to First Set of Interrogatories, at 6.

227 NPS Response to First Set of Interrogatories, at 7.

228 http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapid=7911031 (viewed July 1, 2013); http://www.thefreelibrary.com/Receiver+Appointed+over+the+Assets+of+SLMSoft+Inc.+TSX%3AESP.A+and...-a0131640080 (viewed June 14, 2103).

229 http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapid=7911031 (viewed July 1, 2013).

or license fee should be applied. Third, I consider three quantitative valuation methodologies that are commonly used by economists to value any type of asset (in this case, an intangible asset) and to determine a fair or reasonable fee that a user should pay for access to that asset. These methodologies are the Market Approach, the Income Approach, and the Cost Approach.[230] Fourth, I choose the appropriate reasonable royalty for the patent-in-suit after considering both quantitative and qualitative evidence concerning the value contributed by the patent-in-suit, drawn, in large part, from and consistent with those factors identified in *Georgia-Pacific*.[231]

2. Form of the Royalty

For most real-world licenses and almost all reasonable royalty damages, compensation is provided by one or both of a lump-sum payment and a running royalty fixed to the quantity or revenues associated with the manufacture, shipment, use, or sale of products or services at issue.

A lump-sum typically involves a one-time payment, the magnitude of which is not necessarily directly tied to the extent of alleged usage of the technology at issue by the alleged user/infringer. Some of the perceived implications of a lump-sum damages award have been described by the Federal Circuit as follows:

> A lump-sum license "benefits the patentholder in that it enables the company to raise a substantial amount of cash quickly and benefits the target [*i.e.*, the licensee] by capping its liability and giving it the ability, usually for the remainder of the patent term, to actually use the patented technology in its own products without any further expenditure." … The lump-sum license removes or shifts certain risks inherent in most arms-length agreements. … [A]n upfront, paid-in-full royalty removes, as an option for the licensee, the ability to reevaluate the usefulness, and thus the value, of the patented technology as it is used and/or sold by the licensee. … A licensee to a lump-sum agreement, under usual licensing terms, cannot later ask for a refund from the licensor based on a subsequent decision not to use the patented technology. There is no provision for buyer's remorse.

---

230 *See, e.g.*, Shannon P. Pratt, Robert F. Reilly and Robert P. Schweihs, *Valuing a Business: The Analysis and Appraisal of Closely Held Companies*, 151-258 (McGraw-Hill 2000) ("Pratt, et al. (2000)"); Gordon V. Smith and Russell L. Parr, *Valuation of Intellectual Property and Intangible Assets*, 151-173 (John Wiley & Sons 2000) ("Smith and Parr (2000)"); Robert F. Reilly and Robert P. Schweihs, *Valuing Intangible Assets*, 95-202 (McGraw-Hill 1999) ("Reilly and Schweihs (1999)").

231 *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971).

> The lump-sum structure also creates risks for both parties. The licensed technology may be wildly successful, and the licensee may have acquired the technology for far less than what later proved to be its economic value. The alternative risk, of course, is the licensee may have paid a lump-sum far in excess of what the patented invention is later shown to be worth in the marketplace.[232]

In contrast, a running royalty distributes risk in a different fashion. The Federal Circuit has described a running royalty license as follows:

> In a standard running royalty license, the amount of money payable by the licensee to the patentee is tied directly to how often the licensed invention is later used or incorporated into products by the licensee. A running royalty structure shifts many licensing risks to the licensor because he does not receive a guaranteed payment. Royalties are dependent on the level of sales or usage by the licensee, which the licensee can often control.[233]

In the present case, the appropriate form of relief is a running royalty. A running royalty ties a damages payment directly to the level of infringement. It is a form of payment provided for in the most relevant Fortinet-produced license here. It does not shift risk, as a lump-sum payment does, from one party to another.

3. Royalty Base

In determining an appropriate royalty base, several considerations are often evaluated, including the licensing practices of the patent holder and/or the alleged infringer, the manner in which the alleged infringing products are sold, and the importance of the technology-at-issue.

a. Accused Product Sales

A useful starting point in determining the appropriate royalty base is identification of the "smallest salable infringing unit with close relation to the claimed invention."[234] In the present case, Fortinet has testified that, in the case of hardware products, the smallest saleable unit that incorporates the

---

[232] *Lucent v. Gateway*, 580 F.3d 1301, 1326 (Fed. Cir. 2009).
[233] *Lucent v. Gateway*, 580 F.3d 1301, 1326 (Fed. Cir. 2009).
[234] *Cornell University, v. Hewlett-Packard Company*, 609 F. Supp. 2d 279, 288 (N.D.N.Y. 2009).

technology at issue is an accused Fortinet hardware product, and in the case of accused virtual machines, it is the accused virtual machine.[235]

Mr. Nelson testified that not only is there no smaller "salable unit" that contains just the application layer code used in a FortiOS, but Fortinet does not "sell FortiOS, and we don't sell it in pieces. There's no SKU associated with FortiOS."[236] Mr. Bedwell provided similar testimony, indicating that the FortiOS is not marketed separately from the accused products.[237] Mr. Bedwell testified that "from a marketing point of view I do not separate FortiOS from FortiGate, they are one and the same."[238] He further testified that he did "not know of any way a customer can buy FortiOS. [Fortinet does] not make it available as a standalone product. It ships with the FortiGate or as a FortiGate virtual appliance."[239] Mr. Bedwell also testified that the FortiOS system "[a]bsolutely" differentiates FortiGate products from other competitors.[240] According to Fortinet, FortiOS has not generated revenue by itself.[241] Despite the fact that it does not sell the FortiOS separately, Fortinet does characterize the FortiOS as the foundation for Fortinet's security platforms.[242]

For the most part, Fortinet customers similarly do not have the option of separately purchasing the constituent hardware components of the accused products – such as the proprietary ASICs – as separate components.[243] For certain high-end products, customers are able to purchase some components separately. The FG-5000 systems in the FortiGate line of products, which are targeted towards enterprise level applications, consist of security blades (which are the appliances that operate FortiOS and provide the UTM functionalities) and a chassis (which houses multiple security blades, and optional accessories

---

235 *See*, *e.g.*, Nelson Deposition, at 125, 134; Bedwell Deposition, at 182.
236 Nelson Deposition, at 125, 134.
237 Bedwell Deposition, at 121.
238 Bedwell Deposition, at 121.
239 Bedwell Deposition, at 182.
240 Bedwell Deposition, at 122.
241 *See*, Fortinet, Inc.'s Amended and Supplemental Response to Plaintiff's Interrogatory No. 1, March 4, 2013, at 5; http://www.fortinet.com/sites/default/files/basicfiles/FortiOS_BRO.pdf (viewed June 25, 2013).
242 *See*, Fortinet, Inc.'s Amended and Supplemental Response to Plaintiff's Interrogatory No. 1, March 4, 2013, at 5; http://www.fortinet.com/sites/default/files/basicfiles/FortiOS_BRO.pdf (viewed June 25, 2013).
243 The ASIC processor is not sold separately. *See*, Bedwell Deposition, at 210. Additional hardware accessories are only available for separate purchase on some high-end FortiGate models. *See*, Bedwell Deposition, at 177.

that can expand the number of ports in the FortiGate system).[244] I understand that for these chassis-based systems, only the security blades that run FortiOS are accused products, and the actual chassis and expansion modules that are sold separately for use with the security blades are not accused products.[245]

Including sales of the entire accused product in the royalty base is consistent with Fortinet's own licensing history. As described in the Market Approach analysis below, in a January 2006 settlement and patent license agreement with Trend Micro, Inc. ("Trend Micro"), Fortinet agreed to pay royalties based on revenues from sales of the entire product, rather than on sales of a component part or subset of parts.[246] In a March 2012 settlement and patent license agreement with Brandywine Communications, Fortinet agreed to a lump-sum payment that was calculated based on a royalty rate applied to total sales of the accused products, rather than component parts.[247]

Further supporting consideration of the entire product as the royalty base is, as noted above, evidence that the infringing technology either directly or indirectly influences demand for the infringing products. Although the patented technology is not the sole driver of demand for accused products, it is not a minor feature, such as a "date picker" in a desktop computer operating system. Rather, it contributes to multiple aspects of functionality within the accused products that are highly valued by customers.

Accordingly, when evaluating the quantiative evidence discussed below, I have used as the royalty base the price of the accused Fortinet hardware product or virtual machine that utilizes the FortiOS operating system.

b. Convoyed Sales

According to the Federal Circuit in *Rite-Hite Corp. et al. v. Kelley Co., Inc.,* 56 F.3d 1538 (Fed. Cir. 1995) (*en banc*), damages are awardable on collateral sales if the collateral products are tied functionally to products that compete with those that infringe the patent or patents at issue. Recovery is

[244] Bedwell Deposition, at 177; FORT-NPS 149364-94, at 64, 79.
[245] *See, e.g.*, FORT-NPS 018497-502, at 500.
[246] FORT-NPS 149364-94, at 64, 79.
[247] FORT-NPS 150026-33, at 26, 28.

not allowed, however, where the collateral products are sold with the patented device only as a matter of convenience or business strategy.

Fortinet customers may purchase services, accessories, and complementary products whose use is related to that of the accused Fortinet hardware. Fortinet services include FortiGuard security subscription services, FortiCare technical support services, professional services, and training services.[248] According to Mr. Bedwell, accessories such as "additional storage or certain types of interfaces or ports such as copper or fiber" can be added to high-end FortiGate models.[249] Complementary products include FortiAP, FortiManager, FortiAnalyzer, and the chassis in which the FG-5000 line of FortiGate appliances is mounted.

In determining the extent to which sales of collateral products should be considered in evaluating other licenses here, I consider whether such products are a "functional unit." I also considered Fortinet's licensing practices.

i Functional Unit

(a) Services

FortiGuard and FortiCare

FortiGuard security subscription services provide customers with regular software updates for the application control, antivirus, intrusion prevention, Web filtering, anti-spam, and vulnerability management capabilities on FortiGate appliances.[250] FortiGuard services also provide updates for additional Fortinet products, including FortiClient software, FortiMail, FortiAnalyzer, FortiScan, FortiDB, and FortiWeb appliances.[251] FortiGuard pricing varies depending on the price of the associated hardware, the length of the contract, and the specific functions to which the customer wishes to subscribe.[252] According to Mr. Bray, approximately 70 percent of all of Fortinet's customers purchase

[248] Bedwell Deposition, at 90; FORT-NPS 148967-9079, at 8975.
[249] Bedwell Deposition, at 177.
[250] FORT-NPS 148967-9079, at 8975; Bedwell Deposition, at 34.
[251] FORT-NPS 148967-9079, at 8975.
[252] Bedwell Deposition, at 30-34; Bray Deposition, at 104-06.

FortiGuard as a bundle with antivirus, antispam, intrusion protection and web filtering, [253] although it is possible for some customers to purchase elements of FortiGuard on an a la carte basis.[254]

FortiCare includes technical support services for all Fortinet software, firmware and hardware; premium support services, which provide dedicated support and faster response time, are available to large accounts.[255] As with the FortiGuard services, the range of products for which FortiCare services can be purchased includes both accused and non-accused Fortinet products. FortiCare pricing varies depending on the length of the contract, the price of the associated hardware component and on whether the customer wishes service 8 hours a day x 5 days a week or 24 hours a day x 7 days a week.[256]

In terms of functionality, I understand that FortiGuard and FortiCare services cannot be purchased separately from Fortinet hardware/virtual appliances, and would be of no value to customers without Fortinet hardware/virtual appliances.[257] Although the accused products function without FortiGuard and FortiCare services, as described below, the products and services are promoted together, are typically sold as a bundle, and the majority of customers buy the services alongside the accused products.[258]

When Fortinet promotes FortiGate, it also promotes FortiGuard and FortiCare services.[259] This co-promotion is evident in Fortinet's product data sheets,[260] sales presentations,[261] and white papers.[262] According to the testimony of Mr. Bedwell, the "majority" of customers purchase FortiGuard services.[263]

---

253 Mr. Bray did not know the percentage specifically for FortiGate customers. Bray Deposition, at 24-25.

254 Bedwell Deposition, at 30. According to Mr. Bedwell, when sold separately, web content filtering services are 40 percent of the price of the hardware, antispam services are 25 percent of the price of the hardware, and IPS and application control services are priced at 15 percent of the hardware price. Bedwell Deposition, at 31. When purchased as a bundle, one year subscriptions to FortiGuard services are priced at 45 percent of the list price of the hardware. Bedwell Deposition, at 31; Bray Deposition, at 147.

255 FORT-NPS 148967-9079, at 8975.

256 IN 00008 (Q4-Q9 Americas Price List – 101509.xlsx).xlsx, at 'FortiGate' tab.

257 *See, e.g.*, Bedwell Deposition, at 92.

258 Bedwell Deposition, at 40.

259 Bedwell Deposition, at 92.

260 *See, e.g.* FORT-NPS 000003-09, at 04-06; FORT-NPS000012-13; FORT-NPS 000014-20, at 15.

261 *See, e.g.* FORT-NPS 019393-412; FORT-NPS 019416-40; FORT-NPS 019449-60; FORT-NPS 019461-75.

262 *See, e.g.* FORT-NPS 017383-92; FORT-NPS 017393-400; FORT-NPS 017401-08; FORT-NPS 017409-16.

263 Bedwell Deposition, at 40.

Typically, these services are sold together as a bundle with accused products at the time of purchase.[264] The bundled service contracts can last between 12 and 36 months,[265] with 12 months being the most common term.[266] Customers who do not purchase a service plan bundle automatically receive a three month subscription to FortiCare as part of their purchase.[267] Service plans can be renewed after expiration. According to Mr. Bray, approximately [redacted] of customers who purchase a 12 month service plan renew their subscription.[268]

The functionality of the accused products and FortiCare is closely linked. For example, antivirus, which is a functionality that is updated through the FortiGuard service, is a feature whose use is associated with an infringing configuration of the accused products.

Professional Services

Professional services assist with the design and deployment of Fortinet products in large-scale implementations, and the service staff works with end-customers "to implement [Fortinet] products according to design, utilizing network analysis tools, attach simulation software and scripts."[269]

Fortinet has not produced data showing professional services revenues associated with customers who purchased accused products. According to Mr. Bray, professional services revenues represent less than five percent of Fortinet's overall business, and the revenues are not recorded in a manner that associates them with specific products.[270]

Training

Training services are provided through the Fortinet training department and authorized training partners.[271] Training services include, among other topics, modules directed to the deployment of

---

264 Bray Deposition, at 39.
265 Bray Deposition, at 39-40.
266 According to Mr. Bray, around [redacted] of customers purchase a 12 month service contract. Bray Deposition, at 146-47.
267 According to Mr. Bray, Fortinet attributes a portion of the purchase price of the non-bundled product to the 3-month service, and this is reflected in the service revenue produced by Fortinet. Bray Deposition, at 99-100.
268 Bray Deposition, at 147.
269 FORT-NPS 148967-9079, at 8976.
270 Bray Deposition, at 73.
271 FORT-NPS 148967-9079, at 8975.

FortiGate systems as a transparent application level proxy.[272] Fortinet has not produced data showing training revenues associated with customers who purchased accused products. According to Mr. Bray, training revenues represent a "small" portion of Fortinet's overall service revenues, and represent less than [redacted] of Fortinet's overall business.[273]

(b) Accessories

As noted above, Mr. Bedwell testified that accessories, such as memory and port expansions, are available for high-end FortiGate models.[274] Accessories, including expansion bays,[275] blade modules, power supplies, and fan trays,[276] are all promoted along with FortiGate products. These products are marketed specifically for use with FortiGate products.[277] Blade modules are accessories that are used with the FortiGate-3000 and -5000 product lines. These modules include accelerated interface modules,[278] bypass modules,[279] rear transition modules,[280] security processing modules,[281] and storage modules.[282] These accessories are promoted by Fortinet for use with FortiGate products.[283] Fortinet has

---

272 Bedwell Deposition, at 150-156.

273 Bray Deposition, at 50, 73-75.

274 Bedwell Deposition, at 177.

275 FORT-NPS 000050-53.

276 FORT-NPS 017531-34.

277 http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-5101C.pdf (viewed June 24, 2013).

278 Accelerated Interface Modules increase the flexibility of FortiGate platforms with 10-Gigabit Ethernet and Gigabit Ethernet interface options, and provide wire-speed firewall and near wire-speed IPSec VPN security for traffic traversing the module's ports. Accelerated Interface Modules range in price from $3,000 to $18,000. *See*, http://www.fortinet.com/sites/default/files/productdatasheets/AIM_Module_DS.pdf (viewed June 26, 2013); http://www.avfirewalls.com/AIM-Module-ADM-XD4.asp, (viewed on July 1, 2013).

279 Bypass Modules provide bypass functionality with Ethernet interfaces for protected segments of network traffic, so that modules automatically bridge network traffic in the event of a system failure or power outage. They range in price from $3,000 to $4,000. *See*, http://www.avfirewalls.com/Bypass-Module-ASM-CX4.asp (viewed on July 1, 2013).

280 Rear Transition Modules provide 10-Gigabit Ethernet backplane fabric connectivity to FortiGate and FortiCarrier systems. *See*, http://www.fortinet.com/sites/default/files/productdatasheets/RTM_DS.pdf (viewed June 26, 2013). They are priced at approximately $13,000. *See*, http://www.avfirewalls.com/RTM-XD2.asp (viewed June 26, 2013).

281 Security Processing Modules provide multi-gigabit throughput increases for IPS, firewall, and IP multicast applications. They are in the $10,000 to $30,000 price range. See, http://www.avfirewalls.com/SPModule-ADM-XE2.asp (viewed on July 1, 2013); Fortinet Security Processing Modules Datasheet, SPM-DAT-R3-201004, available from http://www.fortinet.com/sites/default/files/productdatasheets/SPM_DS.pdf (viewed June 26, 2013).

282 Storage Modules add local storage for security and system event logging, and can enable WAN optimization function. *See*, http://www.avfirewalls.com/Storage-Module-FSM-064.asp, (viewed July 1, 2013); Fortinet Storage Modules Datasheet, STORAGE-DAT-R4-201010, available at http://www.fortinet.com/sites/default/files/productdatasheets/FSM-064.pdf (viewed June 26, 2013).

not produced data showing accessories revenues associated with customers who purchased accused products.

(c) Complementary Products

FortiAP

FortiAP appliances are enterprise class, controller-managed wireless access points that extend FortiGate security functions to wireless networks.[284] FortiAP is promoted as "a cost-effective solution for adding WiFi" to a network "[i]f you already have a FortiGate unit."[285] FortiAP sales have totaled approximately [redacted] from July 2004 to December 2012.[286]

FortiGate Chassis

The FortiGate chassis are structures that house FortiGate-5000 series blades. The FortiGate chassis comes in three models, the FG-5020, FG-5050, and FG-5140, which support two, five, or fourteen FG-5000 series security blades, respectively,[287] allowing customers "to scale security and customize [their] unique environment."[288] The chassis are promoted for use with FG-5000 series blades.[289] The FG-5000 series blades may also be used with third-party, industry standard chassis.[290] FortiGate's chassis do not contain software.[291]

Sales of the FG-5020 have totaled approximately [redacted] from July 2004 to December 2012.[292]

FortiAnalyzer and FortiManager

In its latest annual report, Fortinet noted that it "complement[s] [its] FortiGate product line with the FortiManager product family, which enables end-customers to manage the system configuration and security functions of multiple FortiGate devices from a centralized console, as well as the FortiAnalyzer

---

283 *See, e.g.*, FORT-NPS 018078-84, at 82.
284 http://www.fortinet.com/products/fortiap/index.html (viewed June 24, 2013).
285 FORT-NPS 143408-10, at 08.
286 Tab 10.
287 FORT-NPS 000058-61, at 58.
288 http://www.fortinet.com/products/fortigate/5000series.html (viewed June 25, 2013).
289 *See, e.g.*, FORT-NPS 000058-61, at 60; FORT-NPS 017545-48, at 47; FORT-NPS 018078-84, at 80-82.
290 FORT-NPS 148967-9079, at 8974.
291 Nelson Deposition, at 126.
292 Tab 10.

product family, which enables collection, analysis and archiving of content and log data generated by [Fortinet] products."[293] FortiManager and FortiAnalyzer products "are typically purchased to complement a large FortiGate deployment."[294] Fortinet has not produced data showing the magnitude of sales of these products when sold along with accused products.

ii Fortinet Licensing Practices

Fortinet licensing practices as well as industry practices favor including services and accessories related to the accused products in the royalty base. In its agreement with Trend Micro, which is discussed in more detail in the Market Approach section below, Fortinet agreed to pay royalties based on sales of infringing hardware and software products, "essential components that are especially made or especially adapted for" infringing use and not suitable for other uses, and services that are related to infringing use.[295] The terms of the agreement explicitly included hardware products that are accused here, including FortiGate and FortiWifi, and also explicitly included FortiGuard and FortiCare service revenues.[296] Training, professional services, accessories, and other hardware products such as FortiAnalyzer, FortiManager, and FortiAP were not explicitly included in the base.

iii. Convoyed Sales Summary

For the purposes of my calculations, I have provided two royalty bases. One includes accused Fortinet hardware product and virtual machine sales that utilize a FortiOS operating system. The second includes those revenues plus FortiCare and FortiGuard revenues (both bundled revenues and renewal revenues) associated with accused hardware and virtual machine products. I have excluded revenues from professional services, training, FortiAP, FortiGate chassis, FortiAnalyzer and FortiManager from my calculations, but consider these revenues in my evaluation of *Georgia-Pacific* Factor 6.

---

[293] FORT-NPS 148967-9079, at 8971.
[294] FORT-NPS 148967-9079, at 8973. *See also*, Bedwell Deposition, at 107.
[295] FORT-NPS 149927-57, at 29.
[296] FORT-NPS 149927-57, at 47.

c. Sales Summary

The two royalty bases are summarized in Tab 16. As the tab shows, net revenues from U.S. sales of accused products total [redacted] and sales of associated services total [redacted] from the third quarter of 2004 through December 2012.[297]

It is my understanding that accused products sold in Canada and Latin America are tested in the U.S. I have been instructed, therefore, to include sales of these products in my damages calculations. As Fortinet has not produced information regarding its sales of accused products or FortiGuard or FortiCare service revenues in Canada and Latin America, I include estimates of those sales in my analysis. According to Fortinet annual reports, sales in Canada and Latin America were [redacted] of worldwide sales in 2009 compared to [redacted] of worldwide sales in the United States, and Canada and Latin America sales accounted for [redacted] of worldwide sales in 2012 compared to [redacted] for the U.S.[298] Regional sales prior to 2009 were not available.[299] These percentages are consistent with the testimony of James Bray of Fortinet, who testified that Canada accounted for approximately [redacted] of worldwide sales and Latin America accounted for [redacted] of worldwide sales.[300] As summarized in Tab 16, using these percentages, I estimate that Canadian and Latin American sales of accused products total [redacted] and sales of associated services total [redacted] from the third quarter of 2004 through December 2012. If Fortinet produces information showing actual sales in Canada and Latin America, I will update my opinion accordingly.

4. Royalty Payment

As noted above, I typically consider three valuation methodologies that are used by economists to value assets and to determine a fair or reasonable fee that a user should pay for access to those assets.

---

297 Fortinet does not appear to have produced sales of FortiCarrier-branded FortiGate products, which I understand also include FortiOS (*see*, Nelson Deposition, at 194), nor does it appear to have produced bundled service revenues for 2004 through 2005. If such information is produced after the filing of this report, I will update my opinion accordingly.

298 Tab 6.

299 As regional sales were not available prior to 2009, I apply the ratio of Canada and Latin America ("Other Americas") sales to U.S. sales for 2004 to 2008 to estimate Other America sales relative to U.S. sales.

300 Bray Deposition, at 47, 62-63.

These methodologies are the Market Approach, the Income Approach, and the Cost Approach.[301] I describe the evidence from these Approaches in the sections below. I then determine the appropriate reasonable royalty for the patent-in-suit after considering both quantitative and qualitative evidence concerning the value contributed by the patent-in-suit, drawn, in large part, from the factors identified in *Georgia-Pacific*.

a. Market Approach

With Market Approaches, an appropriate price for the use of the patent(s)-at-issue is identified through the examination of the terms of actual transfers of rights (*i.e.*, licenses) involving comparable technology. Inferences are drawn from those comparable transactions to identify terms to which prudent parties would (or should) agree in a hypothetical negotiation in order to permit the alleged infringer to practice the patents-at-issue. [302] In applying the Market Approach, the closer the "other" transactions are in comparability to the hypothetical transaction under consideration, the more useful the information. Past licenses or transactions can differ from a hypothetical transaction in many ways, including:

- parties to the transaction;
- time of transaction;
- nature and scope of the asset/IP transferred (e.g., number of patents, transfer of know-how);
- existing and projected market conditions at the time of the transaction;
- strength of the asset/IP transferred;
- availability and costs of design-around; and
- relative bargaining strength of the parties.

---

301 *See, e.g.*, Pratt, et al. (2000), Smith and Parr (2000), Reilly and Schweihs (1999).

302 If I intend to sell my home over the next year and am seeking to determine a fair price, the Market Approaches suggest that I (or my real estate agent) gather information on other home sales in my neighborhood in the recent past. If four homes have sold for $200,000 in the past year, that information provides strong a priori evidence that my home should be priced at roughly $200,000, with some adjustments upward or downward depending on the characteristics of the houses compared to mine.

In using the Market Approach,[303] the most useful and informative transactions and proposed transactions are those that cover the technology-at-issue or something reasonably close. Other observations unrelated to the patent-in-suit may be associated with a variety of different elements of value and may be of less guidance as to the outcome of the hypothetical negotiation.

i. Quantitative Analysis

(a) Agreements Involving the Patent-in-Suit

As described further below, the patent-in-suit has changed ownership a number of times.

(i) Milkyway Networks Corporation's Purchase of the '601 Patent

On November 17, 1994, Milkyway Networks Corporation entered into an agreement to purchase the application for the '601 patent from its inventor, Hung T. Vu for $1.[304] Mr. Vu was the CEO of Milkyway Networks.[305]

(ii) SLM Networks Corporation's Acquisition of the '601 Patent

On October 1, 1998, the '601 patent was conveyed to SLM by Milkyway Networks Corporation.[306] The patent was acquired as part of the amalgamation of Milkyway Networks Corporation with SLM.[307] Govin Misir was the president of both SLM and Milkyway Networks Corporation at the time.[308]

---

303 The application of the Market Approach in determining reasonable royalty damages is described in *Georgia-Pacific* Factor 1 ("The royalties received by the patentee for the licensing of the patent in suit, proving or tending to prove an established royalty"); *Georgia-Pacific* Factor 2 ("The rates paid by the licensee for the use of other patents comparable to the patent in suit"); and *Georgia-Pacific* Factor 12 ("The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the invention or analogous inventions"). *Georgia-Pacific*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971).

304 NPS0050164-201, at 164.

305 Xie Deposition, at 30.

306 NPS0050166-201, at 166.

307 NPS0050166-201, at 168, 183.

308 NPS0050166-201, at 180-82.

(iii) Bevertec CST, Inc.'s Purchase of the '601 Patent

On February 20, 2004, Bevertec CST, Inc. entered into an agreement to purchase the '601 patent from SLM for $2.[309] SLMSoft was in the midst of bankruptcy proceedings at the time, and Bevertec acquired all the assets of SLMSoft.[310]

(iv) Mount Hamilton Partners, LLC's Acquisition of the '601 Patent

On May 25, 2006, Mount Hamilton entered into an agreement to purchase the '601 patent and its Canadian counterpart from Bevertec.[311] In his deposition, Mr. Ramde was unable to confirm whether the acquisition price was $75,000 or $95,000.[312] The patent had expired because maintenance fees were not paid.[313] However, Bevertec petitioned that the patent be reinstated because the maintenance fees had been missed unintentionally, and the '601 patent was then reinstated and assigned to Mount Hamilton.[314] Bevertec is a company that offers IT recruiting and consulting services to financial institutions and government agencies.[315] As Bevertec is not a manufacturer or distributor of UTM hardware or software, this transaction does not reflect that value of the patent to an entity that manufactures or distributes UTMs.

---

309 NPS0050164-201, at 185. Richter & Partners Inc. was appointed as Interim Receiver and Receiver/Manager of certain undertakings on February 9, 2004 in a court order during SLM's bankruptcy proceedings. *See*, NPS0050164-201, at 185 and 188.

310 NPS0050185-94, at 85 and 88; http://www.bevertec.com/aboutus.htm (viewed June 10, 2013); SLM Networks Corporation is a subsidiary of SLMSoft Inc.. *See*, http://www.thefreelibrary.com/Receiver+Appointed+over+the+Assets+of+SLMSoft+Inc.+TSX%3AESP.A+and...-a0131640080 (viewed June, 14, 2013).

311 NPS0048801-13, at 01-02.

312 Deposition of Rakesh Ramde, June 11, 2013 ("Ramde Deposition"), at 115. Rakesh Ramde indicated that he did not know if Mount Hamilton ever received a signed copy of the agreement, and that it would not surprise him if they had not since the agreement had been faxed back and forth. He indicated that the agreement had been executed. Ramde Deposition at 103-106.

313 Ramde Deposition, at 105-08.

314 Ramde Deposition, at 112-13.

315 http://www.bevertec.com/aboutus.htm (viewed June 10, 2013).

(v) NPS Acquisition of the '601 Patent

On April 30, 2010, NPS entered into an agreement whereby it was assigned the '601 patent from Mount Hamilton Partners, LLC.[316] NPS is a wholly-owned subsidiary of Unified Scientific Advances.[317] Mount Hamilton Partners, LLC is a wholly-owned subsidiary of Innovation Management Sciences.[318] Both Unified Scientific Advances and Innovation Management Sciences are solely owned by Rakesh Ramde and Wilfred Lam.[319] This agreement does not represent an arms-length negotiation between unrelated parties. No consideration was paid in exchange for the patent rights.[320]

(vi) Summary

With the exception of the transaction between Bevertec and Mount Hamilton, these agreements are not arms-length transactions between unrelated parties and, therefore, are of limited probative value here. As the transaction between Bevertec and Mount Hamilton does not reflect the value of the technology to participants in the UTM marketplace, it also provides limited guidance here.

(b) Offers to License Patents in Suit

In December 2006, Mount Hamilton entered into an agreement with IP Value Management, Inc. ("IP Value") to help commercialize the '601 patent.[321] Under the agreement, Mount Hamilton appointed IP Value as its exclusive agent for 90 days, during which IP Value sought to find a buyer for the '601 patent.[322] Mount Hamilton specified that the minimum price that it would accept under this agreement was $1,330,000.[323] The minimum price was determined based on Mount Hamilton's pressing cash needs, and Mount Hamilton's President, Rakesh Ramde, believed the patent was worth more than this minimum

316 NPS00501164-201, at 199-201. Rakesh Ramde could not determine whether Mount Hamilton had paid $75,000 or $95,000, only remembering that it was close to $100,000. Ramde Deposition at 115-116.
317 Ramde Deposition, at 26.
318 Ramde Deposition, at 56.
319 Ramde Deposition, at 26 and 40.
320 NPS00501164-201, at 199-201.
321 NPS0000627-37, at 27.
322 NPS0000627-37, at 28.
323 NPS0000627-37, at 28.

price.[324] IP Value received a $25,000 offer from F5 Networks and a $25,000 offer from Wi-LAN that subsequently expired.[325] IP Value was unable to solicit an offer meeting the minimum price requirement.[326] The commercialization agreement between Mount Hamilton and IP Value was terminated in October 2009.[327]

As these offers do not represent consummated transactions, they are of limited probative value here.

(c) Fortinet Licenses

I have reviewed a number of patent licensing agreements and/or asset purchases produced by Fortinet in this matter.[328]

(i) Agreements in which Fortinet is the Licensee or Purchaser

Agreements in which Fortinet was the licensee or purchaser are summarized in Tab 18.

ClearSwift – Fortinet and Trend Micro – Fortinet Agreements Involving the '600 Patent

In 2004, Trend Micro asserted U.S. Patent Number 5,623,600 (the "'600 patent") against Fortinet in complaints filed with the International Trade Commission ("ITC") and in the Northern District of California.[329] The '600 patent is titled "Virus detection and removal apparatus for computer networks."[330]

---

[324] This sale would have provided Mount Hamilton with at least $1 million, after IPValue's commission was accounted for. *See*, Ramde Deposition, at 178. Mount Hamilton viewed its patent as very valuable; however, after the financial collapse in the fall of 2008, Ramde and Lam, the partners who owned Mount Hamilton, were both in personal financial trouble and faced a large legal bill. *See*, Ramde Deposition, at 178-80; Deposition of Wilfred Lam, June 12, 2013, at 110-11. Because of this, Mount Hamilton was willing to "liquidate" its assets to cover its immediate cash needs, even though it believed the patent was worth more than the liquidation value. *See*, Ramde Deposition, at 180 – 182.

[325] NPS0048471-72, at 71; Mr. Ramde testified that he was "insulted" by the Wi-LAN offer. *See*, Ramde Deposition at 175-76.

[326] NPS0048233-34, at 33.

[327] NPS0048233-34, at 33.

[328] Tab 18.

[329] Federal District Court in the Northern District of California case number C04-01785-RMW and International Trade Commission case number 337-TA-510. FORT-NPS 149256-416, at 325.

[330] U.S. Patent No. 5,623,600. Patents expire 20 years after the filing date. *See*, http://www.uspto.gov/web/offices/pac/mpep/s2701.html (viewed July 3, 2013). The '600 patent filed on September 26, 1995, so it would expire on September 26, 2015. Thus, at the time of the January 2006 settlement agreement, the '600 patent had slightly less than 10 years of patent life remaining.

Trend Micro is a Japanese corporation[331] that provides network security solutions.[332] At the time of the dispute, Trend Micro produced both hardware and software directed towards network security.[333] Mr. Nelson testified that he did not consider Trend Micro a competitor to Fortinet.[334]

In August 2005, the ITC issued a ruling finding that certain FortiGate products infringed the '600 patent, that the '600 patent was enforceable, and that certain (but not all) claims of the '600 patent were not invalid.[335] Concurrent with this finding, the ITC granted an exclusion order barring importation of Fortinet products that practiced the '600 patent from importation into the U.S.[336]

In December 2005, Fortinet entered into an OEM agreement with ClearSwift Limited ("OEM Agreement").[337] The parties also entered into a services agreement on the same date ("Services Agreement").[338] As discussed below, part of the parties' intention in entering into these agreements was to grant Fortinet a sublicense to the '600 patent, which had been the subject of a previous license between a ClearSwift predecessor and Trend Micro.

Under the terms of the OEM Agreement, ClearSwift agreed to license its MIMESweeper software products for incorporation into Fortinet products and to appoint Fortinet an original equipment manufacturer ("OEM") for the delivery, distribution, and manufacturing of its MIMESweeper software when bundled with Fortinet products.[339] As part of this agreement, ClearSwift also granted Fortinet a non-exclusive license to certain ClearSwift intellectual property for use in its capacity as an OEM of Fortinet products bundled with the MIMESweeper software. The license was royalty-free, and the licensed intellectual property included, among other things, all ClearSwift patents, copyrights, mask

---

331 FORT-NPS 149364-94, at 64.
332 http://www.trendmicro.com/us/about-us/index.html (viewed June 12, 2013).
333 http://www.trendmicro.com/cloud-content/us/pdfs/finance/72006q4earningsrelease_perfectfinal.pdf (viewed June 24, 2013); FORT-NPS 146459-576, at 548-51.
334 Nelson Deposition, at 236-37.
335 Limited Exclusion Order, In the Matter of Certain Systems for Detecting Viruses or Worms, USITC Inv. No. 337-TA-510, Aug. 8, 2005; Final Initial and Recommended Determinations, In the Matter of Certain Systems for Detecting Viruses or Worms, USITC Inv. No. 337-TA-510, at 6, 171.
336 Limited Exclusion Order, In the Matter of Certain Systems for Detecting Viruses or Worms, USITC Inv. No. 337-TA-510, Aug. 8, 2005. *See also*, Nelson Deposition, at 234-36.
337 FORT-NPS 149256-416, at 256-75.
338 FORT-NPS 149256-416, at 276-84.
339 FORT-NPS 149256-416, at 256-75.

works, trade secrets and service marks contained in the MIMESweeper software. The intellectual property license was conditional on Fortinet successfully asserting a "summary or other adjudication … as a defense against Trend Micro" in certain disputes pending between Trend Micro and Fortinet. The term of the OEM agreement was five years, and the parties had the ability to renew the agreement for an additional five years.[340]

Under the terms of the OEM agreement, and also conditional on Fortinet's successful adjudication of the disputes with Trend Micro, ClearSwift also granted Fortinet a sublicense to the '600 patent[341] for use with Fortinet products bundled with the ClearSwift MIMESweeper software.

In exchange for the rights received from ClearSwift, Fortinet agreed to pay an initial license fee of [redacted], and, in the event the sublicense to the '600 patent was successfully conveyed to Fortinet, Fortinet agreed to pay ClearSwift [redacted] per year for the sublicense to the '600 patent for the first five years, and [redacted] per year for the following five years, assuming the agreement was renewed.[342] Fortinet also agreed to pay ClearSwift a one-time fee of [redacted] in the event the adjudication regarding the '600 patent was successful.[343] Thus, potential payments to ClearSwift for rights including a sublicense to the '600 patent totaled [redacted] for five years and [redacted] for ten years.

Under the terms of the Service Agreement, ClearSwift agreed to accelerate the packaging and testing of its MIMESweeper product in order to deliver a prototype and completed product. In exchange, Fortinet agreed to pay a total of [redacted] in fees (subject to the completion of certain milestones).[344]

On January 30, 2006, Fortinet announced that it had entered into a settlement and patent license agreement with Trend Micro.[345] The agreement resolved the ITC and district court disputes between the two parties.[346] Under the terms of this agreement, Trend Micro released all claims against Fortinet related to the '600 patent and granted Fortinet a non-exclusive, worldwide license to the '600 patent and

---

340 FORT 149256-416, at 267.
341 FORT-NPS 149256-416, at 256.
342 FORT 149256-416, at 261.
343 FORT 149256-416, at 261.
344 FORT 149256-416, at 276-84.
345 FORT-NPS 149364-94, at 82.
346 FORT-NPS 149364-94, at 82.

all direct and indirect divisionals, continuations, continuations-in-part, reissues, re-examinations and foreign counterparts and equivalents, with no right to sublicense.[347] Both parties entered into a covenant not to sue for any claims related to the '600 patent for a period of five years from the date of the agreement.[348] Fortinet agreed to pay Trend Micro an initial licensing fee of $15.0 million and a royalty payment that was equal to the greater of a minimum quarterly payment or royalty rate as defined below.[349]

Calendar Year	Annual Minimum Payment	Quarterly Minimum Payment	Royalty Percentage
2006 and 2007	[redacted]	[redacted]	[redacted]
2008 and 2009	[redacted]	[redacted]	[redacted]
2010 and 2011	[redacted]	[redacted]	[redacted]
2012 and 2013	[redacted]	[redacted]	[redacted]
2014 and 2015	[redacted]	[redacted]	[redacted]

Thus, Fortinet agreed to a minimum of [redacted], to be paid through 2015, for rights to the '600 patent. Mr. Nelson testified that the [redacted] payment was not the result of a precise formula, but rather the result of a negotiation between the parties taking into a number of considerations including litigation cost, the threat of continued prosecution, and the existing ITC exclusion order.[350]

According to the agreement, royalties are calculated as a percentage of total U.S. sales, net of returns, rebates, credits or taxes of licensed products, and, according to the agreement, the parties agreed that, due to difficulty in tracking the sales of products that infringe the '600 patent, "in exchange for an overall reduced royalty rate, Trend Micro and Fortinet agree that royalties shall be based on the revenues of the Licensed Products without specific determination of infringement by said products."[351] The licensed products that were the subject to these royalty payments included

(a) [H]ardware or software products or systems containing or providing

[347] FORT-NPS 149364-94, at 67, 70.
[348] FORT-NPS 149364-94, at 69.
[349] FORT-NPS 149364-94, at 68, 79-80.
[350] Nelson Deposition, at 255-56.
[351] FORT-NPS 149364-94, at 79. Mr. Nelson testified that the royalty rate was not, in fact, reduced and that the language was included in the agreement at Trend Micro's request. Nelson Deposition, at 259-60.

> computer virus detection and/or elimination functionality to protect a network ("Network Antivirus Functionality"); (b) essential components that are especially made or especially adapted for use in Network antivirus Functionality and not suitable for substantial use other than for use in Network Antivirus Functionality; (c) services for Licensed Products, which services include but are not limited to software subscriptions, renewals and maintenance, related to the detection or elimination of computer viruses to protect a network…[352]

As of the effective date of the agreement, these products included all FortiGate systems, FortiMail-400, FortiMail-2000, FortiWifi-60, the FortiGuard Antivirus Subscription Service, and the FortiCare service for licensed products.[353] The agreement specified that essential components to the licensed hardware or software products include accessories or additions that are specifically designed for antivirus functions, the infringing use in that matter, and are not suitable for other use.

In March 2006, the OEM and Services Agreements were terminated by Fortinet and ClearSwift, citing, in part, Trend Micro's assertion that ClearSwift did not have the right to grant a sublicense to the '600 patent and Fortinet's subsequent settlement with Trend Micro and desire to obtain a license to the '600 patent directly from Trend Micro.[354] Fortinet agreed to pay ClearSwift [redacted] as "full and final payment of all amounts owed under the OEM Agreement and Services Agreement and in consideration for" the terms of the termination.[355]

In late 2008, Fortinet argued that it should not have to continue paying royalties to Trend Micro under the 2006 agreement on the grounds that the Licensed Patent was not valid.[356] This complaint followed a settlement in a separate dispute between Trend Micro and Barracuda Networks, in which Barracuda Networks challenged the validity of the '600 patent in an ITC proceeding.[357] Trend Micro filed a complaint against Fortinet in August 2009 alleging breach of contract and seeking a declaratory judgment that Fortinet was obligated to make certain royalty payments to Trend Micro pursuant to the

---

352 FORT-NPS 149364-94, at 66.
353 FORT-NPS 149364-94, at 84.
354 FORT-NPS 149082-84.
355 FORT-NPS 149082-84, at 84.
356 Complaint for Declaratory Judgment, CV 10 0048, US District Court, Northern District of California, January 6, 2010. *See also*, Nelson Deposition, at 241.
357 Fortinet, Inc.'s Memorandum of Points and Authorities in Support of Its Opposition to Plaintiffs' Demurrers to Fortinet's Third Affirmative Defense, 1:09-cv-149262, April 30, 2010.

January 2006 agreement.[358] In June 2010, Fortinet filed a petition for re-examination of the '600 patent with the USPTO,[359] which led to a May 19, 2011 determination from the USPTO that 35 claims of the '600 patent were invalid and 2 were valid.[360]

On December 21, 2011, Fortinet and Trend Micro entered into a final settlement agreement that resolved all outstanding litigation between the parties and under which Trend Micro released Fortinet from the obligation to pay further royalties as required under the 2006 settlement and licensing agreement in exchange for a one time settlement payment of [redacted].[361] The agreement also clarified that the licensed patents included not only the '600 patent, but also U.S. Patent Number 5,889,943 (a continuation of the '600 patent).[362] Mr. Nelson testified that the [redacted] figure was a negotiated number that did not bear a relationship to sales volumes or a royalty rate and was based on litigation risk, cost of defense, and "a number of other categories."[363]

The series of agreements involving Fortinet and the '600 patent are particularly relevant to the hypothetical negotiation in this matter as 1) they involve a patent that, I understand, is related to a core functionality of Fortinet's products and 2) the licensed products specifically include those at issue in this dispute. Furthermore, I understand that the subject matter of the '600 patent is directed to systems and methods that are comparable or analogous to the technical field of use of the '601 patent.[364] Had the license to the '600 patent been successfully granted by ClearSwift to Fortinet, Fortinet would have paid up to [redacted] for a five-year license, and up to [redacted] for a ten-year license. Although Fortinet received more than rights to the '600 patent under this agreement, ClearSwift also received more than monetary compensation from Fortinet – it also received OEM services and an agreement to have its software incorporated into commercially released product. Had the terms of the initial settlement

358 FORT-NPS 147526-91, at 65.
359 Patrick Bedwell, "Driving a Stake into Security's Innovation Vampire: Exposing the Invalidity of Trend Micro's Patent," Fortinet Security Research (June 2, 2010), http://blog.fortinet.com/driving-a-stake/ (viewed on July 3, 2013).
360 Ex Parte Reexamination Communication Transmittal Form, U.S. Patent and Trademark Office, May 19, 2011.
361 FORT-NPS 149316-63, at 16-18; Nelson Deposition at 243-44.
362 FORT-NPS 149316-63, at 18.
363 Nelson Deposition, at 246-48.
364 Expert Report of Dr. Angelos Keromytis, July 3, 2013.

agreement with Trend Micro been in force through the term of the license, Fortinet would have paid Trend Micro a minimum of [redacted] through 2015. Mr. Nelson testified that under the terms of the original settlement agreement and the final settlement agreement, Fortinet has actually paid Trend Micro in excess of [redacted].[365]

WordCheck Tech, LLC – Fortinet Settlement and Patent License Agreement

On December 23, 2010, Fortinet entered into a settlement and patent license agreement with WordCheck Tech, LLC ("WordCheck").[366] The agreement settled a suit filed by WordCheck in which WordCheck alleged that Fortinet and other parties infringed on U.S. Patent No. 6,782,510 (the "'510 patent"),[367] titled "Word checking tool for controlling the language content in documents using dictionaries with modifiable status fields."[368] Mr. Nelson testified that none of the patents associated with the WordCheck agreement had been found valid and infringed.[369]

I understand that WordCheck and Fortinet are not competitors.[370] Under the terms of the agreement, WordCheck agreed to release all claims against Fortinet related to the '510 patent and granted Fortinet a worldwide, non-exclusive, non-transferable, fully paid-up license to the '510 patent, one additional patent and two patent applications.[371] Fortinet agreed to pay WordCheck a one-time, non-refundable payment of [redacted].[372]

I understand that the patents and patent applications in this agreement relate to a word-checking patent method[373] and, thus, are of limited comparability to the technology at issue here. As such, this agreement provides limited guidance here.

---

365 According to Mr. Nelson, Fortinet made both the $15 million and the $9 million lump-sum payments, and also made the annual minimum payments until it challenged the agreement. Mr. Nelson did not specify the total amount in annual minimum payments made by Fortinet. Nelson Deposition, at 244-246.

366 FORT-NPS 149303-15, at 12.

367 FORT-NPS 149303-15, at 03.

368 FORT-NPS 149303-15, at 14.

369 Nelson Deposition, at 233.

370 Mr. Nelson testified that WordCheck is a non-practicing entity. Nelson Deposition, at 238.

371 FORT-NPS 149303-15, at 14. The additional licensed patent and applications included U.S. Patent No. 7,424,674, titled "Document distribution control system and method based on content", U.S. Patent App. 10/723,370, titled "Email text checker system and method", and U.S. Patent App 12/206,599, titled "Document distribution control system and method based on content."

372 FORT-NPS 149303-15, at 04.

373 Nelson Deposition, at 238.

Brandywine Communication Technologies, LLC – Fortinet Settlement and Patent License Agreement

On March 27, 2012, Fortinet entered into a settlement and patent license agreement with Brandywine Communication Technologies, LLC ("Brandywine").[374] The agreement settled a suit filed by Brandywine on November 2, 2011 in which it alleged that Fortinet infringed on U.S. Patent Number 5,881,142 (the "'142 patent"),[375] titled "Integrated communications control device for a small office configured for coupling within a scalable network."[376] Mr. Nelson testified that none of the patents associated with the Brandywine agreement had been found valid and infringed.[377] I understand that Brandywine is not a competitor to Fortinet.[378]

Under the terms of the agreement, Brandywine agreed to release all claims against Fortinet related to the '142 patent and granted Fortinet and its affiliates and their customers a worldwide, non-exclusive, non-transferable, fully paid-up license to practice the '142 patent in connection with "any past, present, or future product, device, equipment, technology, service, method, system, apparatus, functionality, process, data or content that is made by Fortinet."[379]

The asserted patents did not relate to firewall technologies,[380] and the products that Brandywine alleged infringed on the '142 patent included, but were not limited to, TalkSwitch products that were acquired by Fortinet. TalkSwitch was a company "focused on the development and delivery of VoIP phone systems to companies, home based businesses, institutions and franchises" when it was acquired by Fortinet.[381] TalkSwitch products are now marketed as FortiVoice products.[382]

Fortinet paid Brandywine a settlement payment of [redacted] that reflected "a first-mover

---

374 FORT-NPS 150026-33, at 33.
375 FORT-NPS 150026-33, at 26.
376 U.S. Patent No. 5,881,142. Patents expire 20 years after the filing date. *See*, http://www.uspto.gov/web/offices/pac/mpep/s2701.html (viewed July 3, 2013). The '142 patent filed on July 18, 1995 and will expire 20 years after the filling date, in July 2015. Thus, at the time of the March 2012 settlement agreement, the '142 patent was three years from expiration.
377 Nelson Deposition, at 233.
378 According to Mr. Nelson, Brandywine is a non-practicing entity. Nelson Deposition, at 239.
379 FORT-NPS 150026-33, at 27.
380 Nelson Deposition, at 239.
381 http://www.fortinet.com/press_release/110427.html (viewed June 23, 2013).
382 http://www.fortivoice.com/support/talkswitch-support.html (viewed June 23, 2013).

discount." The total payment was based on a [redacted] percent running royalty rate applied to the estimated revenues of the accused TalkSwitch products through the end of the '142 patent term.[383]

The lump-sum payment in this agreement appears to be based on sales of products that are very different from the products at issue in this matter, and, thus, is of limited probative value here. However, this agreement does indicate that Fortinet has agreed in the past to royalties that were based on total product sales.

Purchase Agreements

Fortinet has produced a number of agreements in which it purchased rights to certain assets, including, but not limited to, patent rights, from third parties, including TalkSwitch Corp., Cosine Communications,[384] Coyote Point, IntruGuard Devices, Inc., IPLocks Japan K.K., Inc., Secure Elements, UTStarcom, WhiteCell,[385] Woven Systems, LLC, and XDN.[386] The dates of these agreements ranged from 2006 to 2012. Each of these agreements involved the payment of a lump-sum by Fortinet to the seller, with lump-sums ranging from $25,000 (purchase of certain equipment from Cosine) to $2.5 million (purchase of all business assets from TalkSwitch).

Among these agreements was a purchase of 26 patent applications (24 U.S., one Japanese and one European) from Cosine Communications for [redacted]. A portion of these purchased patent applications later issued as U.S. patents, and were later asserted by Fortinet against Palo Alto Networks,[387] which I describe further below.

To the extent these purchase agreements reflect value of assets in addition to intellectual property (including the agreements with TalkSwitch,[388] IPLocks,[389] IntruGuard,[390] Woven Systems,[391] Secure

---

383 FORT-NPS 150026-33, at 28.

384 Fortinet entered into a series of transactions with Cosine which ultimately resulted in the purchase of all operating assets of Cosine. Nelson Deposition, at 213.

385 Mr. Nelson testified that the patent purchase from WhiteCell was in the context of "potentially buying their assets." Nelson Deposition, at 177.

386 Tab 18.

387 Nelson Deposition, at 65-66.

388 Tab 18. Mr. Nelson testified that the technology acquired from TalkSwitch is used in Fortinet's FortiVoice product and relates to a telephone system and VoIP PBX. Nelson Deposition, at 227-228.

389 Mr. Nelson testified that the transaction with IPLocks involved the purchase of primarily the operating assets of the company and that some IP did transfer as a result of the agreement. Nelson Deposition, at 218, 227. Mr.

Elements,[392] XDN[393] and Coyote Point[394]), or include consideration in addition to a monetary payment (such as the agreement with WhiteCell, in which Fortinet paid cash plus transferred ownership of certain of its patents to WhiteCell[395]), they are of limited probative value here, as the price paid is impacted by other aspects of the transaction. With respect to the agreements involving only the purchase of patents – UTStarcom and Cosine –Mr. Nelson testified that, at the time of purchase, no analysis of the patents or patent applications purchased from Cosine or UTStarcom relative to Fortinet products was performed, and that he did not have reason to believe the patents were directly applicable to transparent application layer firewalls.[396] Thus, these agreements are of limited value here.

(ii) Agreements in which Fortinet is the Licensor or Seller

Agreements in which Fortinet was the licensor or seller are summarized in Tab 19.

Palo Alto Networks, Inc. – Fortinet Settlement and Patent License Agreement

On January 11, 2011, Fortinet and Palo Alto Networks, Inc. ("PAN") held a mediation to settle litigation related to seven Fortinet-held patents that were allegedly infringed by PAN, as well as claims regarding unfair competition, employee raiding, and breach of contract.[397] PAN is a California-based manufacturer of firewall and UTM hardware[398] and a competitor to Fortinet.[399] Under the terms of the

---

390 Nelson also testified that the IPLocks assets became Fortinet's FortiDB product. Nelson Deposition, at 222.

391 Fortinet purchased all of the tangible and intangible assets of IntruGuard. Tab 18.

392 Fortinet purchased trademarks, URLs, US Patent Applications, Physical Inventory and Equipment and Intellectual Property (including Products, Know-how, designs and code) from Woven Systems. Tab 18. *See also*, Nelson Deposition, at 223, indicating Woven Systems technology was related to a "load balancing product."

393 Fortinet purchased all of the assets of Secure Elements. Nelson Deposition, at 221, 227. The patent assignment agreement did not specify a value specifically attributable to the purchased patents. Tab 18. Mr. Nelson also testified that the Secure Elements assets became Fortinet's FortiScan product. Nelson Deposition, at 222.

394 Fortinet purchased all of the tangible and intangible assets of XDN. Tab 18. Mr. Nelson testified that the XDN technology is used in a redirector service sold by Fortinet and that XDN products are not incorporated into accused products. Nelson Deposition, at 229-30.

395 The Coyote Point transaction was a merger with Fortinet. The Coyote Pointe technology relates to load balancers and is not used in accused products. Nelson Deposition, at 230-231. *See also*, Tab 18.

396 Tab 18. *See also*, Nelson Deposition, at 177-178, characterizing the transaction as trading patents. Mr. Nelson testified that Fortinet did not develop technology based on the WhiteCell patents. Nelson Deposition, at 226.

397 Nelson Deposition, at 209-12, 216-17, 228.

398 FORT-NPS 149986-50015, at 49986; Nelson Deposition, at 166..

399 http://www.paloaltonetworks.com/company/index/ (viewed June 13, 2013).

Bedwell Deposition, at 22.

resulting settlement and patent license agreement, Fortinet granted PAN an irrevocable, worldwide, non-per-unit royalty bearing, non-exclusive, non-transferable/non-assignable license to use the patents to make and sell firewall products, and PAN agreed to pay Fortinet a non-refundable payment of [redacted].[400] The term of the license was for the life of the licensed patents. Fortinet and PAN also released each other from all past or present claims and entered into a covenant not to sue for a period of three years from the date of the agreement.[401]

Mr. Nelson testified that none of the patents associated with the PAN agreement had been found valid and infringed.[402]

As the consideration in this agreement was not limited to patent rights, but also resolved other disputes between the parties, it masks the value associated specifically with the licensed patent rights and is of limited guidance here.

F-Secure OYJ – Fortinet Patent License Agreement

On March 28, 2011, Fortinet entered into an agreement to license rights in a family of patents to F-Secure OYJ ("F-Secure"), a provider of network security software based in Finland.[403] The licensed patents included two patents and five patent applications that had been assigned to Fortinet by WhiteCell Software, Inc.[404] Under the terms of the agreement, Fortinet agreed to grant F-Secure a non-exclusive, non-transferable, non-sublicensable, worldwide, fully paid-up, irrevocable license to practice the licensed patents in relation to F-Secure's software and services, and F-Secure paid Fortinet a fee of $150,000.[405] According to the agreement, Fortinet was "willing to grant the limited license requested by F-Secure…at what Fortinet believes to be a substantial 'first mover' discount and specifically premised upon various

---

400 FORT-NPS 149986-50015, at 49987, 989. The [redacted] was to be paid in one [redacted] installment due within 10 days of the mediation date, followed by twelve payments of [redacted] to be paid prior to the last day of each of the following 12 calendar quarters.

401 FORT-NPS 149986-50015, at 49987, 88, 91.

402 Nelson Deposition, at 233.

403 FORT-NPS 150016-25, at 18; http://www.f-secure.com/en/web/corporation_global/company/vision-and-strategy (viewed June 12, 2013).

404 FORT-NPS 150016-25, at 18, 25.

405 FORT-NPS 150016-25, at 19-20.

important secondary considerations unique to F-Secure."[406]

These "various important secondary considerations" were not specified in the version of this licensing agreement that was produced in this matter.

Mr. Nelson testified that the patents licensed in this agreement were "not specifically" related to firewall technology.[407] This agreement provides limited insight into the outcome of the hypothetical negotiation here.

Sale Agreements

Fortinet has produced a number of agreements in which it sold rights to certain patent rights to third parties, including Cisco, Colorado Remediation, and Tuttle Lane,[408] over the 2011 to 2012 time period.[409]

Cisco paid to Fortinet [redacted] and [redacted] in two separate transactions. The patents sold to Cisco related to virtual routing technology and generally did not relate to UTM or firewall technology, and Fortinet did not do a review of the patents relative to any Fortinet products before selling them to Cisco.[410]

Tuttle Lane paid Fortinet [redacted] in exchange for the assignment of 12 U.S. patents and publications in 3 patent families.[411] Mr. Nelson testified that Tuttle Lane acquired the patents on behalf of Google.[412] The Tuttle Lane transaction included rights to, among other patents, the '311 patent, which had been previously licensed by Fortinet to PAN. Mr. Nelson testified that the patents generally did not relate to UTM or firewall technology, and testified that Fortinet did not do a review of the patents relative

406 FORT-NPS 150016-25, at 18.
407 Nelson Deposition, at 266.
408 Tuttle Lane is also referred to as "AST" in some Fortinet documents. According to Mr. Nelson, the patents were purchased by AST, but Tuttle Lane is the entity AST had take the patent assignment; ultimately, the acquired patents were assigned to Google. Nelson Deposition, at 267.
409 Tab 19. Mr. Nelson testified that some of the patents sold to Google were among those originally purchased from Cosine. Nelson Deposition, at 214-15.
410 Nelson Deposition, at 263-65. Mr. Nelson testified that some of the patents sold to Cisco were among those originally purchased from Cosine. Nelson Deposition, at 214-15.
411 Tab 19.
412 Nelson Deposition, at 185. Mr. Nelson testified that Fortinet received an offer from an un-named non-practicing entity through an intermediary that purportedly exceeded the Tuttle Lane purchase price, but neglected to pursue that offer because it did not want to enter into a transaction with a non-practicing entity. Nelson Deposition, at 183.

to any Fortinet products before selling them to Tuttle Lane.[413]

The agreements with Cisco and the agreement with Tuttle Lane specified that the assigned patents had never been found invalid or unenforceable.[414]

As the technologies transferred in the Cisco agreements and Tuttle Lane agreement appear to not be closely related to the technology at issue here, they are of limited probative value.

The agreement with Colorado Remediation[415] indicated that a material element of the consideration to Fortinet included Colorado Remediation's intent "to commence legitimate business operations focused on vulnerability assessment and remediation technologies, and [the fact that Colorado Remediation] is seeking investment and intellectual property to support this new venture."[416] The agreement also provided for a [redacted] up-front payment to Fortinet, and provided that Colorado Remediation would share with Fortinet 40 percent of the proceeds generated from any monetization[417] of the assigned patents. As the terms of this agreement mask the underlying value of the patented technology, it provides little guidance here.

(d) Market Approach Summary

All but one of the transactions involving a change of ownership of the patent in suit involved related parties and were not arm's-length. The transaction between Bevertec and Mount Hamilton does not reflect the value of the technology as used by a participant in the UTM marketplace.

Based on the terms contained in the licenses produced by Fortinet in this proceeding, running royalty evidence from the Market Approach, primarily from the Trend Micro license, falls in the range of 2.5 to 4 percent for rights to comparable patents, when applied to sales of accused hardware and associated FortiCare and FortiGuard services, with annual minimum payments of between $500,000 and

---

413 Nelson Deposition, at 263-65.

414 FORT-NPS 149800-17, at 03; FORT-NPS 149219-39, at 21; FORT-NPS 149971-85, at 73.

415 Mr. Nelson testified that the IP sold to Colorado Remediation included a group of patent applications which had been purchased from WhiteCell. Nelson Deposition, at 177.

416 FORT-NPS 149677-90, at 77.

417 The agreement defined monetization as any proceeds from reselling, reassigning, licensing, or otherwise deriving any consideration from any portion of the Remediation Patent Family. *See*, FORT-NPS 149677-90, at 78.

$2.0 million and total payments of $24.0 million.

b. Income Approach

The Income Approach provides a systematic framework for estimating the price to be paid for certain intellectual property based on the value of benefits derived from use of the subject technology. The goal of any licensing negotiation is for the parties to find a mutually agreeable way to "share" the benefits from making, using, or selling products embodying the technology at issue. The owner of the technology is entitled to compensation for the portion of the benefits of the product or process that is due to the intellectual property. The licensee should retain certain benefits derived from other attributes of the product or process that incorporate the technology at issue. The licensee should also be compensated for assuming the business risks associated with manufacturing, using or selling the product that embodies the particular technology.

Application of the Income Approach involves two steps. In the first step, the profit rate on products manufactured and/or sold is calculated. In the second step, this profit rate is compared to a "normal" or "benchmark" return (*e.g.*, average returns in the relevant industry), or compared to the return associated with the alleged infringer's next best alternative. Any profits generated on products utilizing the intellectual property that are in excess of the benchmark rate of return or of what the licensee could earn on its next best alternative reflect an amount up to which the licensee should pay for access to the intellectual property. In other words, the incremental return associated with the use of the technology at issue establishes an upper bound on the size of a reasonable royalty that the alleged infringer should be expected to pay (according to the Income Approach).

To the extent the alternative product could not fully replace sales of the accused product, the value of the technology would be even greater than that measured by a comparison of profit rates. A thorough analysis here should examine not only the profit margin differential relative to stand alone Fortinet firewall systems, but also the profits associated with sales that would be forgone entirely absent the alleged infringement.

As all Fortinet UTM products are accused of infringement, there are no non-accused comparable Fortinet products to consider in such a comparison. As it is my understanding that accused products can be configured such that they do not function as a transparent application layer proxy, Fortinet's next best alternative would be to sell accused products with the accused functionality disabled.

Michael Xie, Fortinet's Chief Technology Officer, testified that application processes running in the accused products are "very important" to a UTM firewall "because users expect those features that are offered in this processes [sic]. If they don't run, the user wouldn't get what they want"[418] and that if none of the application processes are running, "the FortiGate wouldn't offer any features that [sic] I wouldn't think anybody would use them."[419] Based on Mr. Xie's testimony, it appears that only customers who did *not* use the accused functionality in the actual world would continue to purchase accused Fortinet products in the but-for infringement world. Thus, the Income Approach would involve comparing Fortinet's profits from sales of accused products to profits from the sales level it would be able to achieve absent use of the accused technology.

As summarized in Tab 16, sales of accused products and associated bundled services and renewals total approximately [redacted] in the U.S. and [redacted] in Canada and Latin America from July 2004 through December 2012. According to Mr. Xie, the "majority of the Fortinet customers who purchase the FortiGate product, when they use them, they would use at least one of the application processes that running [sic] on the FortiGate product."[420] As Mr. Xie did not quantify the precise percentage of FortiGate customers who use application processes, I assume that "the majority" equates to at least 50 percent. Thus, by disabling the accused technology, Fortinet might stand to lose at least [redacted] in revenues in the sale of accused products and service revenues that are directly tied to those sales.[421] To the extent sales of other products that are used in conjunction with accused products – such as FortiAnalyzer and FortiManager – would also be lost, this figure underestimates foregone revenues.

---

418 Xie Deposition, at 96-97.
419 Xie Deposition, at 98-99.
420 Xie Deposition, at 98.
421 As Tab 16 shows, net revenues from accused products and services in the U.S., Canada, and Latin America totaled approximately [redacted].

To calculate the profit associated with these revenues, I estimate Fortinet's incremental profit margin. I treat Fortinet's cost of goods sold ("COGS") as fully variable. Fortinet's COGS are summarized in Tab 5, and average approximately [redacted] for products and approximately [redacted] for services over the 2004 to 2012 period.[422] The weighted average gross profit margin over the 2004 to 2012 period, based on actual sales of accused products and associated software, is [redacted].[423]

To determine variable operating (or non-manufacturing overheard) expenses, I examined how operating expenses[424] vary with activity level. A common tool used by economists to determine the relationship between two values is called a regression analysis. The regression analysis is designed to measure the degree to which a dependent variable (in this case, operating expenses) changes in relation to a given change in an independent variable (in this case, sales). These changes represent the incremental change in operating expenses associated with an incremental change in sales.[425] In employing a regression analysis here, I used an ordinary least squares analysis to determine the historical relationship between Fortinet's operating expenses and its sales.[426]

As a check on the regression results, I employed two alternative methodologies. For the first alternative method—the High-Low Method—I have examined sales and operating expenses data for Fortinet's highest sales year and its lowest sales year over the relevant period.[427] For the second alternative method —the Increment Method—I have examined year-to-year changes in Fortinet sales and operating expenses to determine the historic relationship between changes in sales and changes in costs.[428] The results of these three methodologies are summarized in Tab 25. The regression method gives an estimate of incremental operating expenses of 45.5 percent; the two alternative methodologies yield

---

422 According to Fortinet, it "does not track cost or profit information on a per-product basis." Fortinet Inc.'s Objections and Responses to Plaintiff Network Protection Sciences, LLC's Fifth and Sixth Sets of Interrogatories, June 3, 2013, at 7. Therefore, I use gross profit margins as reported by Fortinet in its SEC filings for products and services. *See*, Tab 5. The margins shown in Tab 5 are roughly consistent with the testimony provided by Mr. Bray regarding Fortinet's products. Bray Deposition, at 143, 170-73.

423 Tab 20.

424 Here, I include SG&A and R&D in the calculation of operating expenses.

425 The inclusion of an operating cost in this analysis does not indicate a conclusion that the cost is variable or fixed. Rather, it is the results of the analysis that give that indication.

426 Tabs 21 and 22.

427 Tab 23.

428 Tab 24.

estimates of incremental operating expenses of 46.1 percent to 38.4 percent of sales. I use the median of these three methods as the incremental operating cost percentage.[429] The incremental profit rates in each year from 2004 to 2012 are summarized in Tab 26.

As summarized in Tab 27, the application of this incremental profit rate to the revenues that would be foregone results in [redacted] in profits that would be foregone over the period July 2004 to December 2012 if Fortinet disabled the technology at issue in the accused products. As a percent of the smaller royalty base described above, that is [redacted].[430] As a percent of the larger royalty base described above, that is [redacted].[431]

c. Cost Approach

The Cost Approach involves an examination of the costs required to construct or purchase an alternative technology that performs the same function as the patented technology, but which does not infringe the patent or patent-in-suit.[432] The cost to construct a non-infringing alternative technology is also called "design-around cost." According to the Cost Approach, a user of certain patented technology would pay no more for access to that technology than its avoided costs.

Often times, a Cost Approach focuses on avoided out-of-pocket capital expenditures. However, such examinations tend to underestimate the true value of assets, including intellectual property assets. To appraise the value of a house, one could examine the replacement costs associated with bricks, mortar and lumber. These costs, however, do not measure the value of the house or its fair price. Purchasers pay amounts substantially in excess of out-of-pocket brick, mortar and lumber costs. That is because the total value generated exceeds the accounting or out-of-pocket costs of the inputs. According to Reilly and Schweihs:

---

429 Tab 25.

430 Calculated from Tab 27. Net sales of accused hardware and virtual machines total [redacted].

431 Calculated from Tab 27. Net sales of accused hardware and virtual machines and associated service revenues total [redacted].

432 Reilly and Schweihs (1999), at 97.

> Costs describe what the intangible asset owner spent in the original production process, or what the owner would have to spend as of a certain date to recreate that production process. Cost, by itself, does not tell us how much a buyer would pay to acquire the intangible asset, or how much a seller would seek to motivate the sale of the intangible asset…
>
> Value is not necessarily equal to cost, at least not to cost as measured in the historical accounting sense. Rather, value is equal to cost measured in the economic sense. The economic measure of cost is usually equal to an accounting measure of cost that has been adjusted by either (or both) incremental and decremental influences caused by market conditions.[433]

The "economic" facts that need to be considered include the costs of unsuccessful design attempts, the period of the design-around, and the going forward impacts of the alternative.

Out-of-pocket costs of a design-around are relevant only if the alternative is acceptable – technically, commercially and financially. Avoided costs associated with alternatives that are unacceptable provide little or no indication of value. If the alternative is acceptable, but not available in the relevant timeframe, then the out-of-pocket costs must include the costs associated with the delay in implementing the alternative technology. In situations in which such a delay is unacceptable, then, again, the avoided costs provide little or no indication of value.

Here, I have not seen sufficient evidence to quantify the Cost Approach.

d. Summary of Quantitative Approaches

The Market Approach indicates a running royalty based on a percent of total accused hardware, virtual machine, and associated service revenues of 2.5 to 4 percent and indicates annual payments of between $500,000 and $2 million per year. The Income Approach indicates disabling the accused functionality would be associated with foregone profits of at least $56.2 million, which equates to approximately 12.4 percent of a sales base that includes accused hardware, virtual machines, and associated services revenues. The Cost Approach provides no additional information.

[433] Reilly and Schweihs (1999), at 97, 121.

e. Qualitative Factors

In addition to the quantitative evidence, qualitative factors should be (and are) considered in evaluating the Market, Income, and Cost Approaches and the hypothetical negotiation. The relevant qualitative factors emanate from *Georgia-Pacific.*[434]

Georgia Pacific Factor 1 – The royalties received by the patentee for the licensing of the patent in suit, proving or tending to prove an established royalty.

I have not seen any agreements in which SLM Networks or others who owned the patent have licensed rights to the patent-in-suit in an arm's-length deal to third parties who participate in the UTM marketplace. Transactions in which the patent in suit changed ownership are discussed above. Thus, this factor has a neutral effect on the royalty rate.

Georgia Pacific Factor 2 – The rates paid by the licensee for the use of other patents comparable to the patent in suit.

As noted above in the Market Approach, Fortinet has produced information regarding a number of licenses and purchase agreements. Of the agreements involving only the transfer of intellectual property rights, it is my understanding that the Trend Micro agreement involves technology that is most comparable to the patent-in-suit.

In its 2006 agreement with Trend Micro, Fortinet agreed to pay [redacted] for past sales and a running royalty ranging from [redacted] percent of hardware and service revenues for future sales, with annual minimums ranging from [redacted] from 2006 to 2015.[435] In 2011, the agreement was amended and Fortinet agreed to pay a one-time lump-sum fee of [redacted].[436]

This information is already taken into consideration in the Market Approach.

---

[434] *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116 (S.D.N.Y. 1970), modified and aff'd, 446 F.2d 295 (2d Cir. 1971).

[435] FORT-NPS 149927-57, at 931 and 942-943.

[436] FORT-NPS 149879-926, at 880.

Georgia Pacific Factor 3 – The nature and scope of the license, as exclusive or non-exclusive; or as restricted or non-restricted in terms of territory or with respect to whom the manufactured product may be sold.

(i) Scope of IP Covered by License

All else equal, a license that includes rights to a variety of patents, copyrights and know-how is more valuable than one that does not (*i.e.*, a "naked" license). The hypothetical license construct used to assess reasonable royalty damages presumes a naked license that provides the licensee (*i.e.*, the alleged infringer) with permission to practice the patent-in-suit. It does not provide for the transfer of any know-how, technical assistance or any other intellectual property rights from the patent holder/licensor to the alleged infringer/licensee.

Here, the Trend Micro agreements included rights to the '600 patent as well as a continuation patent (as well as foreign counterparts), both of which represent a narrow set of IP rights, as is the case with the hypothetical license.[437] Thus, no additional adjustment is required here in relation to that agreement.

(ii) Exclusivity

The hypothetical license construct used to assess reasonable royalty damages presumes a non-exclusive license, as it is intended to provide the hypothetical licensee only with the right to *use* the technology at issue and not, for example, the right or ability to prevent other parties from practicing the technology.[438] Moreover, the patent owner cannot and should not be effectively constrained by the hypothetical license from suing or licensing any other party it deems appropriate under its patents.

Here, the hypothetical license would be non-exclusive. The Trend Micro agreement provided for

---

[437] Conversation with Dr. Angelos Keromytis, June 7, 2013.

[438] In *Mobil Oil Corp. v. Amoco Chemicals Corp.*, 915 F. Supp. 1333 (D. Del. 1994), the court noted that "[a] patent owner may recover as a measure of damages the royalty rate established by prior actual licenses for acts comparable to those engaged in by the infringer without authority." In its decision, the court drew a parallel between the hypothetical license and a non-exclusive license, noting that "[t]he rights needed by Amoco to use [the infringing] process are similar to the rights granted to the ... licensees" which was a "non-exclusive license." The court also wrote that "[t]he rights infringed by Amoco were similar or 'comparable' to the rights granted under the standard license."

non-exclusive rights to the licensed patents, and thus no further adjustment for exclusivity is required here.

(iii) Legal Strength of IP

A patent that has been judged valid, enforceable, and infringed, or that has been readily acknowledged by the industry as such, is generally worth more than a patent for which these issues are still in doubt.

In the hypothetical negotiation construct, it is appropriate to assume that the patent-in-suit is valid, enforceable and infringed, and that both parties are aware of these facts.

The 2006 agreement between Trend Micro and Fortinet was entered into after a finding that most of the asserted claims of the ’600 patent were not invalid, and after a finding of infringement (and associated exclusion order) by the ITC. The 2011 amendment was entered into after a finding of validity with respect to certain claims by the USPTO. In all, this factor is already taken into consideration and has no incremental effect on the outcome of the hypothetical negotiation relative to the rates provided for in those agreements.

Georgia Pacific Factor 4 – The licensor’s established policy and marketing program to maintain his patent monopoly by not licensing others to use the invention or by granting licenses under special conditions designed to preserve that monopoly.

A hypothetical negotiation is assumed to be conducted in an environment in which the patent holder is essentially *required* to grant the alleged infringer permission to practice the patent-in-suit in exchange for compensation adequate for the alleged infringer’s unauthorized use of the patent-in-suit.

In the present case, I am not aware of any policy of SLM Networks or NPS regarding the granting of licenses to patented technology. This factor has a neutral effect on the outcome of the hypothetical negotiation.

Georgia Pacific Factor 5 – The commercial relationship between the licensor and the licensee, such as, whether they are competitors in the same territory in the same line of business; or whether they are inventor and promoter.

When licensing to a direct competitor, a licensor may demand a relatively high royalty rate because, by granting a license, the licensor risks losing sales and market presence to the licensee.

At the time of the hypothetical negotiation and at the time of its acquisition of the patent-in-suit, SLM apparently was not involved in the business of manufacturing or selling UTMs or firewalls.[439] As such, SLM Networks did not directly compete with or envision competing with Fortinet in the marketplaces for the accused products.

When considered relative to the Trend Micro agreement, no further adjustment is necessary as Mr. Nelson testified that he does not consider Trend Micro and Fortinet to be competitors.[440] Moreover, a hypothetical negotiation presumes a willing licensor and willing licensee.

Georgia Pacific Factor 6 – The effect of selling the patented specialty in promoting sales of other products of the licensee; the existing value of the invention to the licensor as a generator of sales of his non-patented items; and the extent of such derivative or convoyed sales.

In some instances, sales of products embodying the patented technology enhance the sales of related goods and services. The existence of such sales, referred to as tag-along or convoyed sales, increases the value of the protection provided by the hypothetical license.

As noted above, in the present case, Fortinet enjoys convoyed sales in the form of FortiGuard and FortiCare services, which are included in the larger royalty base, as well as sales of other products that are not included in either royalty base, including professional services, and training courses related to the purchase of accused products, as well as the sales of related products, such as the FortiAP, FortiGate

[439] SLM was a subsidiary of SLMSoft, Inc., a company that developed software for online financial transactions. *See*, http://www.siliconinvestor.com/readmsg.aspx?msgid=4239187 (viewed July 1, 2013); http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=7911031 (viewed June 25, 2013).

[440] Nelson Deposition, at 236-37.

Chassis, FortiManager, FortiAnalyzer, and accessories to the FG-5000 series security blades that operate in concert with infringing products running the FortiOS operating system.[441]

Using the smaller royalty base would suggest an upward impact to the rate in the Trend Micro Agreement because of the convoyed sales. Using the larger base suggests no change to the Trend Micro Agreement for that reason above.

Sales of other products not included in either royalty base appear to be significant. Although Fortinet has not provided data sufficient to quantify the magnitude of sales of the FortiManager and FortiAnalyzer, it has characterized both products as complements to the FortiGate product line and ranks both among its "core product(s)."[442] Training and professional services represent less than 5 percent of Fortinet's total revenues.[443] Net revenues of the FortiAP and FortiGate 5020 chassis total over [redacted] in the U.S. from 2004 through 2012.[444]

The negotiating parties would be aware of the magnitude of these convoyed sales. This factor would tend to put upward pressure on the royalty rate relative to the Income Approach, as profit from sales of such products are not included in that calculation. With respect to the Trend Micro agreement, sales of such products do not appear to have been included in the royalty base, but, as the parties are likely to have been aware of the value of the sales of such products, that value is likely reflected in the rate. Thus, no additional adjustment is required here relative to the Market Approach.

Georgia Pacific Factor 7 – The duration of the patent and the term of the license.

The patent-in-suit will expire on November 21, 2014.[445] Accordingly, at the time of the hypothetical negotiation in May 2002, the patent-in-suit would have retained a significant portion of its patent life. There is no evidence in this case regarding an appropriate method to adjust for the duration of

---

441 FortiGate FG-5000 security blades function with the FortiGate chassis, but they may also be used with third-party chassis. *See*, FORT-NPS 148967-9079, at 974.

442 FORT-NPS 148967-9079, at 8971-75.

443 Bray Deposition, at 50, 73-75.

444 Tab 10.

445 U.S. Patent No. 5,623,601. Patents expire 20 years after the filing date. *See*, http://www.uspto.gov/web/offices/pac/mpep/s2701.html (viewed July 3, 2013). The '601 patent was filed on November 21, 1994, so it will expire on November 21, 2014.

the patent or term of the license.

Georgia Pacific Factor 8 – The established profitability of the product made under the patent; its commercial success; and its current popularity.

As a general matter, greater commercial success of the accused products will tend to increase the amount that should be paid for access to the patent-in-suit. In the present case, the determination of the commercial success and popularity of the accused products can be assessed based on their actual market acceptance (*i.e.*, sales and profitability).

Fortinet's sales of accused products and related services have been substantial. Between July 2004 and December 2012, net sales of accused hardware products and associated FortiGuard and FortiCare services in the U.S. totaled over [redacted] and have totaled an estimated [redacted] in Canada and Latin America.[446]

According to Fortinet and Mr. Bray, Director of Finance and Treasury at Fortinet, Fortinet's overall worldwide gross profit margin is typically [redacted] for products and typically [redacted] for services.[447] Mr. Bray testified that profit margins in the U.S. and profit margins specific to accused product are typically similar to the worldwide aggregate.[448]

As the magnitude of sales of accused products and associated profits is taken into consideration in the Income Approach, no additional adjustment is required here.

Relative to the Trend Micro agreement, the commercial success and profitability of the accused products has a neutral effect on the hypothetical negotiation, as the licensed products in that agreement include the products at issue here.

---

446 Tab 16.

447 Bray Deposition, at 1, 143, 170-73.

448 According to Fortinet, it "does not track cost or profit information on a per-product basis." Fortinet Inc.'s Objections and Responses to Plaintiff Network Protection Sciences, LLC's Fifth and Sixth Sets of Interrogatories, June 3, 2013, at 7; Bray Deposition, at 143, 170-73.

Georgia Pacific Factor 9 – The utility and advantages of the patent property over the old modes or devices, if any, that had been used for working out similar results;

and

Georgia Pacific Factor 10 – The nature of the patented invention; the character of the commercial embodiment of it as owned and produced by the licensor; and the benefits to those who have used the invention.

It is my understanding that firewall technologies prior to the technology at issue include packet filter firewalls, deep packet inspection firewalls, and explicit proxies.[449] According to Dr. Keromytis, relative to transparent application layer proxies, such technologies are either less effective at identifying threats, or are associated with a loss of transparency in order to achieve enhanced effectiveness.[450] As discussed above, it is my understanding that a transparent application proxy represents an improvement over prior firewall technologies because 1) it offers application level data inspection, which accurately reconstructs information coming through the firewall in a manner that allows the firewall to more effectively block the passage of unwanted data relative to other methods of doing so, and 2) it is transparent in that it does not require the system to be separately configured by a user or system administrator in order to accommodate each individual user and host in the protected network that wishes to traverse the firewall in accessing the public network.[451]

As discussed above, evidence that I have reviewed indicates that the ’601 patent both directly and indirectly influences demand for the accused products. Mr. Xie, Fortinet’s Chief Technology Officer and Vice President of Engineering, testified that the ability to run application-layer services was critical to demand for FortiGate UTMs,[452] and Mr. Bedwell testified that some of the application-layer services “are extremely important for customers” and they “can be the reason they bought our FortiGate versus

[449] Conversation with Dr. Angelos Keromytis, June 7, 2013.
[450] Conversation with Dr. Angelos Keromytis, June 7, 2013.
[451] Conversation with Dr. Angelos Keromytis, June 7, 2013.
[452] Xie Deposition, at 91,98-99.

somebody else's."[453] Several marketing materials mention application-layer services.[454] From among the many capabilities that FortiGate appliances offer, these same marketing materials also feature antivirus,[455] antispam,[456] DLP,[457] and SSL-encrypted traffic inspection,[458] which, I understand, practice the '601 patent when used on an appliance running the FortiOS operating system.[459] This indicates that these are viewed as significant features of the FortiGate products by Fortinet and its customers, and is evidence of the '601 patent's indirect effect on demand for the accused products.

Market assessments have also pointed to the benefits that are both directly related to the '601 patent and related to features that practice the '601 patent. A 2010 review of Fortinet products by The 451 Group noted Fortinet's expanded application-layer security;[460] a 2012 Frost & Sullivan report indicated that "Fortinet offers a strong value proposition of comprehensive network security in a single, easily deployed network appliance…FortiOS is the operating system that powers all FortiGate® security products and each FortiGate device includes the full suite of security technologies" including antispam, and DLP, among other features;[461] and a 2010 Frost & Sullivan review of the global UTM market described Fortinet as the leader in the UTM market and stated that its market strategy was to offer "a broad suite of security technologies, such as firewall, VPN, IPS, antimalware, antispam, and Web content filtering, that when combined constitute a comprehensive threat management solution."[462] A January 2013 Current Analysis report identified the combination of multiple security features, including antivirus,

---

453 Bedwell Deposition, at 115.

454 *See*, *e.g.*, FORT-NPS 064422-24, at 23; FORT-NPS 064346-48, at 47; FORT-NPS 064317-19, at 19; FORT-NPS 064392-94, at 93; FORT-NPS 017383-92, at 88-90; FORT-NPS 019179-86, at 86.

455 For examples of product reviews, *see* FORT-NPS 060512-13; FORT-NPS 061740-41. For examples of sales presentations, *see* FORT-NPS 017417-54; FORT-NPS 017834-53; FORT-NPS 017938-52. For examples of data sheets, *see* FORT-NPS 000003-09; FORT-NPS 000025-31; FORT-NPS 000050-53.

456 For examples of product reviews, *see* FORT-NPS 061740-41. For examples of sales presentations, *see* FORT-NPS 017417-54; FORT-NPS 019476-516; FORT-NPS 019593-636. For examples of data sheets, *see* FORT-NPS 000025-31; FORT-NPS 000050-53; FORT-NPS 017809-14.

457 For examples of sales presentations, *see* FORT-NPS 019476-516; FORT-NPS 019593-636; FORT-NPS 017938-52. For examples of product data sheets, *see* FORT-NPS 000025-31; FORT-NPS 000050-53; FORT-NPS 017809-14.

458 For examples of sales presentations, *see* FORT-NPS 017834-853. For examples of product data sheets, see FORT-NPS 000025-31; FORT-NPS 017809-814; FORT-NPS 000003-09.

459 Conversation with Dr. Angelos Keromytis, June 7, 2013.

460 FORT-NPS 145513-14, at 13.

461 FORT-NPS 146991-97, at 93.

462 FORT-NPS 146680-774, at 752, 753.

DLP, and antispam, as one of Fortinet's strengths,[463] and a November 2010 Current Analysis report noted that DLP and SSL inspection were two of the "four major new capabilities" that were added to Fortinet's FortiOS 4.0 upgrade "along with hundreds of other improvements."[464]

The profit advantages from selling products incorporating the patented technology are reflected in the Income Approach, discussed above. This factor provides no additional guidance in that respect.

These factors are already taken into consideration in the Market Approach, as I understand the patents in the Trend Micro agreement are of comparable importance to the patent in suit.

Georgia Pacific Factor 11 – The extent to which the infringer has made use of the patent; and any evidence probative of the value of that use.

As Tab 16 shows, from July 2004 through December 2012, Fortinet sold approximately [redacted] in accused products and associated services in the United States and an estimated [redacted] in Canada and Latin America.[465] U.S. sales of the accused products and associated services accounted for approximately one-half of Fortinet's total U.S. revenues. On a worldwide basis, U.S., Canada, and Latin America sales of accused products and associated services account for approximately [redacted] of total Fortinet reveneues.[466] Fortinet characterizes the FortiGate appliances as its "flagship" products.[467]

Relative to the agreement with Trend Micro, this factor has a neutral effect, as the licensed products in that agreement included FortiGate, FortiCare, and FortiGuard. Information relevant to this factor has already been taken into consideration in the evaluation of the Income Approach.

[463] FORT-NPS 145497-501, at 497.
[464] FORT-NPS 145503-12, at 04.
[465] Tab 17.
[466] Tab 17. Fortinet did not report total U.S. revenues in its SEC filings prior to 2009.
[467] FORT-NPS 148967-9079, at 8974.

Georgia Pacific Factor 12 – The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the patent or analogous patents.

I have not seen information regarding a customary split of profit in the UTM industry. Thus, this factor has a neutral effect on the outcome of the hypothetical negotiation.

Georgia Pacific Factor 13 – The portion of the realizable profit that should be credited to the invention as distinguished from non-patentable elements, the manufacturing process, business risks, or significant features or improvements added by the infringer.

Although the '601 patent contributes critical functionality to the accused products,[468] there are a number of other aspects of accused product functionality not covered by the '601 patent. In particular, Fortinet marketing materials for the FortiGate promote its proprietary ASIC processor,[469] as well as features and capabilities such as web filtering, WAN optimization, application control, VoIP security, vulnerability management, and, in the case of higher end, chassis-based models, scalability.[470] Product reviews also mention the ASIC processor in FortiGate appliances along with other, non-infringing capabilities.[471] In addition to the ASIC, other non-accused hardware components contained within accused products, but, in most cases, not sold separately, include connecting ports,[472] such as high speed Ethernet ports, user-definable 10/100 ports, DMZ ports, and USB ports,[473] and local storage.[474] Some

---

468 Conversation with Dr. Angelos Keromytis, June 7, 2013.

469 *See, e.g.*, FORT-NPS 000050-53, at 50.

470 *See, e.g.*, FORT-NPS 000050-53, at 52; FORT-NPS 018497-502, at 497; FORT-NPS 017523-26, at 23; FORT-NPS 017545-48, at 45; FORT-NPS 017519-22, at 19; FORT-NPS 017531-34, at 31.

471 *See, e.g.*, FORT-NPS 060512-13; FORT-NPS 061736-37; FORT-NPS 061740-41.

472 Certain connecting ports are not available on all models. DMZ ports are not available on FortiGate-50 and lower models. See, FORT-NPS 061168-71, at 68.

473 *See, e.g.*, FORT-NPS 062384-87, at 84; FORT-NPS 061168-71, at 68, 70; FORT-NPS 061558-61, at 60; FORT-NPS 018186-92, at 92.

474 Among the currently marketed models, local storage is not available on FortiGate-60 and lower models. *See, e.g.*, http://www.fortinet.com/sites/default/files/basicfiles/ProductMatrix.pdf (viewed June 26, 2013). In some previously marketed versions of the FG-50 and -80 series appliances, optional, internal memory was included in the FG-51 and FG-81 appliances. *See*, FORT-NPS 000014-20, at 15; FORT-NPS 000023-24, at 23.

models include the option to install expansions that add additional ports and memory.[475]

Other accused products include additional functionality above and beyond that included in standard FortiGate products, such as VoIP gateway, IP PBX, router and switch functionality in the FortiGate Voice and FortiWiFi Voice; and 802.11a/b/g/n wireless access point (WiFi) functionality in the FortiWiFi and FortiWiFi Voice.

As there are other non-accused elements of value not included in this estimate, this factor suggests substantial additional downward pressure on the royalty relative to the Income Approach.

This factor was likely to have been incorporated in the bargaining between Trend Micro and Fortinet, as the patent in that agreement covered only a portion of the functionality in the licensed products (which explicitly included FortiGate, FortiWifi, FortiGuard and FortiCare). Thus, this factor provides no additional information when evaluated relative to that agreement.

Georgia Pacific Factor 14 – The opinion of qualified experts.

I have reviewed the opinions of Dr. Angelos Keromytis, and they are included in the discussion of the products and technology.

Georgia Pacific Factor 15 – The amount that a willing licensor would have agreed to accept, and that a willing licensee would have agreed to pay at the time the infringement began.

I have considered qualitative factors that should influence the royalty in my analysis of the *Georgia-Pacific* factors. Although some factors provide upward pressure and others provide downward pressure, this analysis generally suggests neutral pressure relative to the royalty payments considered under both the Market and the Income Approaches.

The Market Approach indicated a running royalty based on a percent of total accused hardware, virtual machine, and associated service revenues of 2.5 to 4 percent for rights to comparable patents, and indicated annual payments of between $500,000 and $2.0 million per year. The majority of the *Georgia-Pacific* factors are neutral relative to this evidence, as the Trend Micro agreement already reflects

[475] *See, e.g.*, FORT-NPS 018120-21; FORT-NPS 017979-80.

consideration of these factors.

The Income Approach indicated disabling the accused functionality would be associated with foregone profits of at least $56.2 million, which equates to a royalty of 12.4 percent.[476] Factor 6 indicates upward pressure relative to the Income Approach, as the Income Approach does not include sales and profits associated with products such as FortiManager and FortiAnalyzer, which are sold along with accused products. Factor 13 indicates downward pressure relative to the Income Approach, as there are a number of non-accused elements of value that are not quantified in the Income Approach. The Cost Approach provided no additional information.

Based on my analysis of the evidence from the Market Approach, Income Approach, and Cost Approach, and application of the *Georgia-Pacific* factors a running royalty of 4 percent of sales is appropriate here.[477] When applied to U.S. sales of accused hardware and virtual machines, damages total $6.8 million; when applied to U.S. sales of convoyed sales of bundled services and service renewals, damages total $6.4 million.[478] Damages associated with estimated sales in Canada and Latin America total $2.4 million for accused hardware and virtual machines and $2.4 million for convoyed sales of bundled services and service renewals.[479] Total damages when applied to sales of accused hardware and virtual machine and associated services in the U.S., Canada, and Latin America are $18.1 million.[480] The damages amount assumes a finding of liability for the patent-in-suit.

V. PREJUDGMENT INTEREST

Courts allow injured parties to receive prejudgment interest on damage awards in order to compensate successful plaintiffs for the passage of time. The appropriate interest rate is one that fairly compensates the plaintiff for the time value of money while properly accounting for risk in a financial

---

476 Calculated from Tab 27.
477 Tab 3.
478 Tab 3.
479 Tab 3. Calculations based on estimated sales in Canada and Latin America. If Fortinet produces information regarding actual sales of accused products and associated services in Canada and Latin America, I will update my calculations accordingly.
480 Tab 3.

sense. Should the Court determine that prejudgment interest is due after a judgment is entered in this case, the appropriate interest rate to use is the short-term Treasury Bill rate.

This relatively low, mostly riskless rate is the appropriate rate because it conforms to the fundamental tenet of finance that investors who bear less risk should earn lower profits, or returns. Conversely, higher returns accrue to investors that bear higher risk. Since NPS in this case bears virtually no risk that Fortinet cannot pay the judgment (*i.e.*, there is virtually no default risk), the correct interest rate is a low, relatively risk-free rate.

In Tab 28, I have summarized the prejudgment interest factors that should be applied to the damages award. These calculations assume a damages award on September 28, 2013. I will update these calculations and calculate prejudgment interest in preparation for trial.

VI. CONCLUSION

Based on my analysis of the evidence from the Market Approach, Income Approach, and Cost Approach, and application of the *Georgia-Pacific* factors, it is my opinion that NPS is entitled to reasonable royalty damages based on a running royalty rate of 4 percent. When applied to U.S. sales of accused hardware and virtual machines, damages total $6.8 million; when applied to U.S. sales of convoyed sales of bundled services and service renewals, damages total $6.4 million.[481] Damages associated with estimated sales in Canada and Latin America total $2.4 million for accused hardware and virtual machines and $2.4 million for convoyed sales of bundled services and service renewals.[482] These amounts assume a finding of liability for at least one claim of the patent-in-suit. Total damages when applied to sales of accused hardware and virtual machines and associated services in the U.S., Canada, and Latin America are $18.1 million.[483]

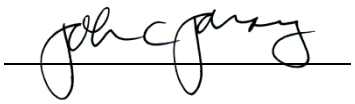
---

[481] Tab 3.

[482] Tab 3. Calculations based on estimated sales in Canada and Latin America. If Fortinet produces information regarding actual sales of accused products and associated services in Canada and Latin America, I will update my calculations accordingly.

[483] Tab 3.

The opinions expressed herein are based on the information that was available to me as of the date of this report. If additional information is provided to me subsequent to the filing of this report, I may revise, supplement or expand my opinions prior to trial, if necessary.



John C. Jarosz